Channel Futures™

CLOUD BACKUP AND DATA PROTECTION

The Easiest Way for VARs to Generate Services Revenue

POWERED BY | Acronis

INTRODUCTION

Disruption is the new normal. The digital transformation juggernaut continues to redefine virtually all phases and facets of global business, including the value-added reseller (VAR) segment. Forces including the cloud, exploding device adoption and data growth, an ever-diversifying array of software-as-a-service solutions (targeting an ever-diversifying array of business cases) and innovations in automation are radically reshaping the VAR model, calling into question what role the category serves and how it will define success in the decade ahead.

Credit forward-looking VARs for adapting to these sweeping changes, albeit slowly. Many have added recurring licenses, SaaS solutions and cloud infrastructure to their product portfolios — a significant step in the right direction.

But there's so much more still to be done in a world where organizations decisively favor renting IT services from expert providers over owning and operating technologies internally. New, "everything-as-a-service" startups are multiplying across the competitive landscape and reinventing the go-to-market formula with dizzying speed. VARs must evolve with them… or else.

As the pages to follow demonstrate, embracing this increasingly lucrative "as-a-service" approach to offer cloud backup and data protection services represents a VAR's most direct path to sustained success and growth. Those with the best hopes for flourishing in 2020 and beyond will manage an increasing number of cloud services, leverage automation tools to support their customers and relentlessly explore new ways to maximize the numerous platforms sprouting across the tech ecosystem — including platforms complete with automation offerings that help VARs efficiently move up the stack to higher-value services. There are also new managed services platforms that handle critical operational details, security updates, infrastructure management and routine tasks.

With the right platform approach in tandem with a curated list of solutions, VARs can offer their customers and partners managed services without the friction and expense synonymous with building an entirely new business model or business unit. Here's how.

The Business Case for Adding Higher-Value Services

There are any number of compelling reasons prompting VARs to expand their recurring higher value services and managed services offerings. Some — like overall business stability and predictability from recurring revenue versus sporadic purchases, as well as increased profitability — are rather obvious.

More to the point, however, VARs who stay the course and offer only traditional license renewals, support and service contracts and basic managed services space are increasingly vulnerable. Embracing cloud services safeguards VARs against obsolescence: cloud is the fastest-growing IT services segment, with Gartner forecasting the worldwide public cloud services market will increase from $182.4 billion in 2018 to $331.2 billion in 2022[i] as enterprises forgo traditional services and adopt a "cloud-first" mentality when selecting IT products and services.[ii]

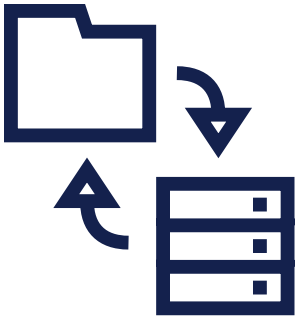
IT Services: TOP 5 and BOTTOM 5

by CAGR % (2017-2022)

Source: Gartner Webinar; Top Trends Driving Change for IT Services

Top 5	CAGR % 2017-2022
IaaS	**26.6**
Infrastructure Utility Services	**14.1**
Mobile (Managed Workplace Services)	**11.3**
Colocation	**11.0**
Hosting	**10.4**

Bottom 5	CAGR % 2017-2022
Desktop (Managed Workplace Services)	**-3.5**
Hardware Support (Client Device Support)	**-3.4**
Service Desk Outsourcing	**-3.2**
Data Center Outsourcing	**-2.5**
Enterprise Network Ousourcing	**-2.3**



The managed cloud services sector is no stranger to exponential growth, either, with the worldwide market on pace to reach $84.7 billion by 2023, more than doubling from $41.4 billion in 2018. [iii] Gartner anticipates that cloud-related services like consulting, implementation, migration and managed services will account for 28 percent of total cloud budgets by 2022. [iv]

Bottom line: VARs that want to improve their business metrics and grow from both a mid- and long-term perspective must bulk up their managed cloud services portfolio. The world is turning to the cloud — and turning away from VARs that don't follow suit.

Building and Managing a Cloud Service Portfolio

How does a VAR make the leap forward? Managed cloud services begin with two core elements. The first is a **platform** for service management, onboarding, integration and customization.

Building a service management platform is a complex and daunting software development effort, which is why VARs (as well as MSPs) are better off working with a technology partner that provides a robust, tested, pre-packed solution — for example, the **Acronis Cyber Cloud.** A service provider-optimized platform allows partners and VARs to quickly package and offer cloud services with little or no upfront costs, and the best platforms enable the creation of differentiated services, allow for the tweaking of business and pricing models, and the integration of cloud services into their portfolio.

Regardless of the provider, a cloud managed services platform must deliver the following capabilities:

- Multi-tenancy with secure service partition to support multiple customers
- Ability to create various offerings and service bundles

- Single sign-on for customer accounts and integration to external SSO systems
- A policy engine that supports customized usage and security policies such as role-based access controls (RBAC)
- Usage quotas
- Multiple payment models such as pay-as-you-go, annual subscriptions, reserved capacity, etc.
- Unified management console that supports multi-tenant environments
- Extensive usage reporting, auditing, metrics and dashboards
- Integration with other systems including user provisioning, user authentication/IAM, billing/accounts payable, ticketing/support, CRM
- Personalized branding (i.e., a white-label offering)
- A REST API that facilitates the development and integration of custom cloud-based services

Managed cloud success also hinges on a thoughtfully curated **collection of services.** Sure, a VAR could continue selling hundreds of solutions from hundreds of vendors. But it makes far more sense to simplify, identifying a handful of vendors that will address all your needs — specifically, vendors in dedicated niches (e.g., networking, data protection, IaaS, infrastructure management, productivity tools, etc.) that offer mission-critical services like:

- Endpoints (desktops, laptops and mobile devices)
- Internet and mobile data services
- VOIP services
- Printers
- Email and office productivity apps (Office 365 or Google Apps)
- CRM apps
- Finance apps
- ERP/HCM apps
- Marketing apps
- Endpoint management (mobile and desktop/laptop)

Acronis is a veritable Swiss army knife for cyber protection. It won't cover 100 percent of your cloud services needs — no single vendor will — but it will address a significant chunk of them, including:

- Data protection services
- Business continuity
- Endpoint security solutions (e.g., ransomware protection)
- File storage and sharing
- File certification, verification and e-signing services

Whatever verticals a VAR chooses to serve, there are Acronis solutions that will add value to their clients.

Data Protection: The Foundation of a Cloud Services Portfolio

It's always a healthy business strategy to pursue products and services categories with a large total available market (TAM), and Data Protection-as-a-Service (DPaaS) fits the bill perfectly, with IDC anticipating the market will grow at a 16.2 percent CAGR through 2022, climbing to $10.2 billion.[v]

A compelling data protection services portfolio starts with **secure backup** for data on traditional servers and enterprise storage arrays, along with IDC anticipating the market will grow at a 16.2 percent CAGR through 2022, climbing to $10.2 billion.[v] virtual machines, virtual storage environments and cloud-based resources. A product like **Acronis Cyber Backup Cloud** enables VARs to securely store all of an organization's critical data assets using a hybrid storage design that supports both on-premises and cloud-based storage, and it doesn't lock customers into a single location or environment.

Disaster recovery (DR) services, another critical component of a comprehensive VAR data protection offering, extend backup with the ability to quickly recover data and restart applications on secondary infrastructure (typically a cloud recovery site).

The process automation traditionally required for a failsafe DR service can require a significant amount of software development — an effort VARs can sidestep by using a SaaS product like **Acronis Cyber Disaster Recovery Cloud**, which adds DR to their cloud service portfolio. The turnkey product supports both physical and virtual workloads, provides a GUI editor for creating DR automations and can test various recovery scenarios without disrupting production systems.

Next, **file sync, sharing and storage** deliver the cloud-based file sharing capabilities enterprises demand, complete with security, business controls and data protection. While some consumer services offer an enterprise version, these are generally standalone products that do not pair favorably with other data protection and security services an enterprise might use. Instead, VARs can offer a complete, integrated solution by incorporating **Acronis Cyber Files Cloud**, a customizable service that works with existing storage systems or cloud infrastructure from Acronis. Like consumer services, it supports mobile devices, Windows PCs, Macs and all popular web browsers, but also provides enterprise-friendly features like in situ editing for Microsoft Office documents.

Then there are must-haves for the paperless office: **file certification, verification and e-signing** capabilities offer a secure, irrefutable mechanism for approving digital documents and validating their authenticity. A product like **Acronis Cyber Notary Cloud** allows VARs to deliver a blockchain-based service for file notarization, e-signing and verification and enables customers to authenticate documents and meet regulatory requirements for data integrity and transparency.

And as far as healthy business strategies go, data protection services time and again prove themselves **the easiest sale a tech provider can make.** In fact, many of today's largest MSPs got their start offering backup, DR and security solutions, then "landing and expanding" from there.

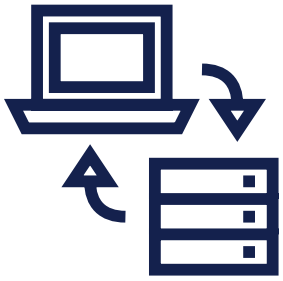
Going Beyond Data Protection to Stay Competitive

Traditional challenges like power outages and natural disasters are not the only dangers facing business in the 21st century, of course. Cyber threats pose enormous danger to organizations across the globe. According to Accenture,[vi] digital security breaches have increased 67 percent in the last five years, rising 11 percent in the last year alone.

That's bad news for business — and good news for VARs. In a world where $2.9 million is lost to cybercrime every minute,[vii] VARs gain a substantial competitive advantage by evolving from traditional, commodity backup products to comprehensive cyber protection offerings. Acronis describes cyber protection as a new generation of data protection that converges with cyber security and goes beyond to address all five vectors of what the company calls **SAPAS**. VARs can build differentiated, secure data protection services for their customers by leveraging these components.

The SAPAS acronym begins with **safety**, i.e. ensuring that unadulterated copies of data are always available. It also encompasses **accessibility** to enable today's mobile, always-online customers and employees to access and use corporate data from anywhere, as well as **privacy** measures to ensure that sensitive, confidential data is kept out of the prying eyes of unauthorized individuals (while providing the necessary controls for legitimate users). No less vital is **authenticity**, to guarantee that data hasn't been surreptitiously altered and that legitimate copies are identical to the original.

Last but certainly not least, VARs must offer **security** solutions to protect data, systems and users from malicious actors — both external hackers and internal rogue employees. Security must cover both data at rest (stored) and in motion (over the network) using various techniques like encryption, hashing, digital signatures, monitoring and attack prevention and remediation.



VARs and MSPs offering an integrated suite of secure data protection services must also account for ransomware protection. Ransomware (a type of malware that blocks access to computer systems and data, restoring access only when owners pay a ransom to the malware operators) is projected to strike a business every **14 seconds by the end of 2019;**[viii] attacks on business targets already surged 195 percent from the fourth quarter of 2018 to the first quarter of 2019, according to a Malwarebytes report. [ix]

Acronis Active Protection stops ransomware from encrypting and disabling files, backups and even the backup software itself, continually monitoring file accesses and changes to identify and thwart potentially harmful activity before a ransomware attack can wreak havoc. And in case ransomware manages to get through the defense, Acronis Active Protection restores encrypted files automatically, saving service providers a huge amount of time on recovery and minimizing downtime. Because it is integrated into Acronis Cyber Backup Cloud, this technology instantly reduces exposure to ransomware for you and your customers without installing anything else on top of your backup agents.

Delivering Cyber Protection with Acronis

Acronis Cyber Cloud doesn't stop at providing backup, DR, file sync-and-share, document notarization and data security. It also integrates with core MSP/CSP back-office tools — for example, Service Management, Ticketing, Monitoring and Alerting — to make MSPs more efficient.

Moreover, Acronis Cyber Cloud is the *only* solution that offers both a set of in-demand cyber protection services and a platform for provisioning and user management, granting service providers the latitude to promote their brand and own the customer relationship. Acronis Cyber Cloud also supplies access to Acronis' cloud infrastructure and support for private systems for service delivery.

Partner roadmap: How to start selling Acronis Cyber Cloud

By building its portfolio on a solid SaaS foundation from an established software vendor, a VAR can offer cloud services with **minimal upfront investment in time or money**, along with the support of a partner with deep-rooted expertise in secure data protection.

On top of technical expertise, a cloud services vendor must provide comprehensive sales and marketing support through its partner program. Acronis cloud partner program experts assist VARs across all service lifecycle stages, from the initial kickoff (where Acronis helps the VAR navigate everything from service launch to pricing and packaging development) to customer onboarding to ongoing marketing campaigns and pre-sales support.

Secure Data Protection Services: Examples and Use Cases

The secure data protection capabilities offered via Acronis Cyber Cloud enable VARs to market a wealth of generic and customized cloud services designed to appeal to organizations of all shapes and sizes. The most popular categories include:

Multi-faceted **hybrid data protection services** that work with any infrastructure, including local servers or storage arrays, VAR-managed systems in a colocation facility or cloud storage resources. A typical deployment scenario uses a cloud service for the primary archive, with optional secondary copies to local storage. Such hybrid deployments allow VARs to provide the cloud service and cross-sell hardware-software bundles to handle local storage.

The growing popularity of SaaS applications like Office 365 presents another situation ripe for cloud services using a solution like Acronis Cyber Backup Cloud. Many VARs are offering a **bundle of Office 365 and a Backup solution,** which assists their customers of meeting their data protection goals and in some cases compliance requirements.

SaaS data protection services can be extended with **cloud file sync and share services** to enhance collaboration while maintaining controls over data exfiltration and unauthorized access.

Cloud-based DR services extend data archive services with process automation that can restore disrupted operations to provider-managed remote locations and eliminate an organization's need for costly, redundant infrastructure. From a long-term perspective, as customers adopt cloud infrastructure to host enterprise applications, VARs can extend the service to use IaaS resources as the DR location.

Converged data protection — security services address the ransomware scourge that holds an organization's valuable data hostage. Such data disablement illustrates the inadequacy of traditional malware-based defenses and highlights the need to combine data protection and security monitoring under a symbiotic service umbrella. Many traditional, signature-based anti-virus solutions have become defenseless, and now modern solutions protect data with technology like Acronis Active Protection, which employs sophisticated machine learning models to detect and stop ransomware, allowing VARs and

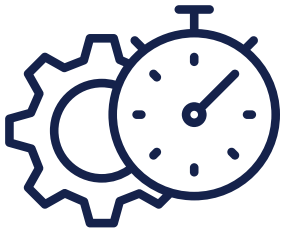
MSPs to deliver state-of-the-art security services while leaving the complex implementation and management to a third-party expert.

Partners and VARs can also extend and customize these generic, foundational services with features targeted to particular industries and customers. An extensible and white-labeled platform like the Acronis Cyber Cloud suite ensures that partners have full control over branding, customizations and the customer relationship. VARs and MSPs can extend the capabilities of the Acronis Cyber Cloud suite with the **Acronis Cyber Platform**, which provides a series of APIs and SDKs; in addition, customization and extension allow VARs and MSPs to create unique offerings that differentiate their brand from the competition.

Popular areas for targeted services include **workstation backup to the cloud,** as well as **long-term archival with vaulted storage** to lower-cost, cold storage cloud services for regulatory compliance.

Another booming opportunity: **healthcare**, which requires HIPAA-compliant storage and backup. **One MSP specializing in services for dentists** used the built-in AES-256 encryption of Acronis Cyber Backup Cloud to deliver a HIPAA-compliant service while saving $30,000 versus its previous backup software. And after a **leading provider of automated practice management (PM) and electronic health records (EHR) solutions** switched to Acronis Cyber Backup Cloud, it reduced recovery time by 90 percent while exploiting the scalability of cloud services to increase its customer base by tenfold over two years.

Still another can't-miss proposition: cyber protection targeting **retail, logistics, and insurance** — verticals with a distributed network of branch offices they're struggling to centrally manage and protect. The Acronis platform provides these businesses:



- Centralized cyber protection for all branch offices, with centralized backup policy and self-service recovery.
- Remote recovery capabilities, including centralized automated remote recovery.
- One-click recovery automation that doesn't require IT personnel.
- No required capital equipment investment for branch offices — all services run in the cloud.
- Single-pane-of-glass administration for servers, workstations and Office 365.

Recommendations and Call to Action

Secure cloud data protection services offer VARs significant opportunities to grow high-margin recurring revenue and dazzle and retain customers. Partnering with an established software provider like Acronis to build a service portfolio allows VARs to focus on what matters: with Acronis in its corner, a VAR can direct its energy towards service **differentiation and customization,** as well as **improving margins through lower overhead.** It can also **address new and evolving threats like ransomware, accelerate the pace of service development** and deployment, and **cross-sell related products and services.** Most of all, a VAR can **develop a strong brand that engenders customer loyalty and reduces churn.**

Contact Acronis Sales for a business discussion and a live product demo.

CONTACT US

Sources

[i] Gartner. “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019.” Press Release. April 2, 2019.

[ii] Gartner. “Top Trends Driving Change for IT Services.” Webinar. March 25, 2019.

[iii] IDC. “Worldwide Managed Cloud Services Forecast, 2019–2023: An Extraction View of Technology Outsourcing Services Markets.” Market Forecast. September 2019.

[iv] Prabha, Anil. “Public Cloud Services Market to Hit $214bn.” TechHQ, April 8, 2019.

[v] IDC. "Worldwide Data Protection as a Service Forecast, 2018–2022: Initial Market Sizing." Market Forecast. July 2018.

[vi] Accenture. Ninth Annual Cost of Cybercrime Study. March 6, 2019.

[vii] “Cybercrime Costs Global Economy $2.9m Per Minute.” Infosecurity Magazine. July 24, 2019.

[viii] Morgan, Steve. “Global Ransomware Damage Costs Predicted to Hit $11.5 Billion by 2019.” Cybercrime Magazine, November 17, 2017.

[ix] Zamora, Wendy. “Labs Cybercrime Tactics and Techniques Report Finds Businesses Hit with 235 Percent More Threats in Q1.” MalwareBytes, April 25, 2019.