



Acronis



WHITEPAPER

# The Five Levels of MSP Platform Integration

How MSPs can efficiently leverage integrated cyber protection services to make money and grow by protecting customer systems, applications and data

# Introduction

MSPs trying to build a highly profitable, growing, low-churn business face a variety of obstacles. For starters, many providers have built a multi-service offering slowly over time, cobbling together a patchwork of service delivery infrastructure from a collection of disparate vendors. The resulting lack of integration adds complexity from both a business and operations standpoint, carrying high costs and making service expansion more difficult over time.

**Cybersecurity services** are one of the most obviously promising paths to MSP growth and increased profits right now. The world is awash in cyberthreats like ransomware attacks, and every business (especially in the small-to-medium sector) is struggling to avoid the costly downtime and data loss they inflict. It might be tempting for an MSP to bolt a few cybersecurity point products onto its existing service suite. But that only increases the infrastructure heterogeneity problem, with the resultant drag on profits and efficiency worsening with the addition of each new service.

**There is a better way** to address the urgent need of SMBs for cyber protection services while also achiev-

ing steady, profitable growth. But to do so, MSPs must address five distinct, critical challenges of integration and automation at the operational and technological level. This paper examines these challenges and considers how MSPs might address them.



*“The benefits of working with Acronis are very clear: it is easy to use, making it easy to recover VMs or physical machines thereby providing the business continuity that CUT requires.”*

**Michael Edmunds,**  
**Head of Partner Marketing, Bastion**  
**Backups**

# Statistics show businesses are struggling with cyber protection and basic IT operations

Any operator who spends much time talking with their customers understands that implementing and maintaining cybersecurity is one of their biggest business challenges, and that they can't find the staff they need to address it.

## Independent market research bears out these findings:

- Average time between availability of a patch and its installation: 102 days (*Ponemon Institute: 2018 State of Endpoint Security*)
- Average annual staff productivity lost to IT downtime: 545 hours (*ERS IT Solutions, 2019*)
- Average time spent resolving one incident of IT downtime: 200 minutes (*ERS IT Solutions, 2019*)
- Average cost per endpoint of a successful cybersecurity attack: \$470 (enterprise) to \$763 (SMB) (*Ponemon*)

These issues are only projected to get worse, as cybersecurity job vacancies are forecast to swell to 3.5 million openings worldwide by 2021, per Cybersecurity Ventures.

## This provides enormous opportunities for any MSP that can step into that breach with a suite of cyber protection services, including:

- Cross-sales of cyber protection services to existing customers
- The ability to “land and expand”, winning new customers with core offerings and later growing those accounts by adding cyber protection services, and
- Further “land and expand”, starting with one popular application (e.g., Office 365) and expanding cyber

protection to other applications (e.g., back-office finance and accounting) and to new platforms (like mobile devices, servers and cloud storage and backup)

Reaping the highest yield from this fertile field, and then growing those yields year after year, requires a smarter approach based on five levels of MSP platform integration. The ability to close new customers, grow business with existing ones and minimize churn – all while reducing capital and operating costs to improve margins – rests on the ability to improve integration at the business, product, management, user-interface and technology levels. Let's look at each of these in turn.

SMB struggles with cybersecurity issues will only worsen as cybersecurity job vacancies swell to 3.5 million openings worldwide by 2021, per Cybersecurity Ventures



# Level 1: Business integration

Cyber protection services are obviously attractive, but they only become profitable if they can mesh neatly with your existing service delivery infrastructure as well as existing business systems. Adding a new vendor to your mix for every new service you offer costs you money at every step of your business process.

## **BUSINESS INTEGRATION CHALLENGE:**

Suites of services built on heterogeneous infrastructure from multiple vendors increases the cost and complexity of service packaging and bundling, integration with billing and provisioning systems, marketing program development and delivery, and vendor contract/SLA negotiation and management.

## **BUSINESS INTEGRATION SOLUTION:**

One common, integrated platform for services delivery that simplifies bundling, integrates seamlessly with back-office systems, enables unified marketing messaging, and collapses the number of vendors you have to manage.

## **BUSINESS INTEGRATION BENEFITS:**

Simpler, easier sales and marketing with faster lead velocity, higher-margin service delivery, and lower vendor management costs.



## Level 2: User interface (UI) integration

The UI integration challenge is simple but profound: more panes of glass equals higher data center power, cooling and real-estate costs, higher training costs for your techs, more complexity for them to manage, and a greater chance that critical alerts will be missed.

### UI INTEGRATION CHALLENGE:

Managing a miscellany of vendor point products requires multiple panes of glass and the development of non-reusable skills for each technology.

### UI INTEGRATION SOLUTION:

One integrated management console with a uniform user interface that is optimized for IT operations and supports professionals' workflow across the entire services suite.

### UI INTEGRATION BENEFITS:

Faster and more cost-effective training, more efficient operations, and improved job satisfaction among IT techs through the use of more operator-friendly tools.



## Level 3: Management integration

New services don't exist in a vacuum. You need to be able to provision them, remotely monitor and manage their performance at the customer site, capture information from them for trouble-ticketing purposes, patch and upgrade them, and bill the customer for them.

In an ideal world, you can add more functionality and capabilities to them at the application programming interface (API) level. The more seamlessly they mesh with your existing management systems, the less costly they are to operate, and the higher the margins they deliver.

### MANAGEMENT INTEGRATION CHALLENGE:

Lack of integration with a variety of systems (including RMM, PSA, and third-party cybersecurity products) leads to costly manual operations and limits product expansion.

### MANAGEMENT INTEGRATION SOLUTION:

Unification of the management of policy, auditing, access and privacy controls, tightly coupled with existing ticketing, alerting, and RMM systems. Adoption of systems with APIs and integration points that are simple to deploy and enable the use of custom security controls for access control and other group-based and individual security policies.

### MANAGEMENT INTEGRATION BENEFITS:

More efficient, higher-margin services delivery with the potential to expand cyber protection services via platform API integration.



*"Integrations to the ConnectWise platform are extremely important to our MSPs. The integration between Acronis Cyber Cloud and ConnectWise Control is the first such integration. It looks fantastic and our MSPs find a ton of value in it."*

**Jeff Bishop,**  
Chief Product Officer, ConnectWise

# Level 4: Product integration

There's a stark contrast between offering a suite of services built on multiple standalone products and one built on a platform where turning on a new service is a mere question of software enablement.

Where you once needed a utility belt studded with a flip-phone, GPS device, flashlight, camera, and so on, you now need just a smartphone. It is compact, cost-effective, easy to secure, manage and operate, and easy to upgrade with new applications. MSPs need a similarly integrated, platform-based approach at the product level.

## PRODUCT INTEGRATION CHALLENGE:

Building suites of services with multiple vendor point products can create stubborn technology problems, including interoperability issues. Adding and bundling new services becomes more expensive and complex to manage, provision, bill for and report on. Adding new products becomes increasingly difficult and costly for your IT staff to manage, limiting opportunities to serve new customer requirements and compete with new market entrants.

## PRODUCT INTEGRATION SOLUTION:

One platform that enables delivery of a complete set of cyber protection services: backup, disaster recovery, file sync and share, AV, anti-malware, vulnerability assessment, patch management, and a diverse range of storage targets.

## PRODUCT INTEGRATION BENEFITS:

Ability to offer a broad range and flexible mix of data protection and cybersecurity services to address a variety of business use-cases without the cost and complexity disadvantages of a heterogeneous, multi-vendor infrastructure. Additional benefits include more granular integration of and information exchange between products, e.g., the ability to scan backup archives stored in the cloud to ensure they are malware-free before using them for recovery.

**Average Endpoint**

- 1 x CPU
- 8 GB RAM
- Windows 10
- 1 TB local storage
- Office 365
- Six additional apps

**IT OPERATIONS/  
CYBERSECURITY  
MANAGEMENT  
FUNCTIONS**

**OS:** policies, patching, vulnerability, configuration management

RMM, behavioral anti-malware, backup / data protection, signature-based anti-virus, cloud data, network management

# Level 5: Technology integration

The ability to remotely manage a suite of services on your customer's virtual machines (VMs), servers, desktops and mobile devices requires some level of local-agent real estate.

A proliferation of agents, each managing a discrete service, presents a raft of problems: adverse performance impact on endpoints, the potential for interoperability and resource conflicts between agents, lack of integrated alerting and reporting, and a reduced ability to efficiently and cooperatively exploit automation technologies like orchestration, machine learning (ML) and artificial intelligence (AI).

## TECHNOLOGY INTEGRATION CHALLENGE:

Multiple endpoint agents from multiple vendors can create performance and interoperability problems, inhibit automated responses based on alerts, ML/AI and integrated data flows, and require more manual operations.

## TECHNOLOGY INTEGRATION SOLUTION:

One agent on the endpoint to enable the delivery of a suite of cyber protection services (e.g., backup, AI-enhanced behavioral anti-malware protection, and endpoint management) and additional automation features.

## TECHNOLOGY INTEGRATION BENEFITS:

Faster deployment, simplified management and maintenance, fewer performance and interoperability issues, and more highly-automated event response.

*"We wanted to consolidate to a single technology with centralized manageability for all of our clients and be able to monitor and manage everything from a single interface. We really just needed to be able to manage everything in one place."*

**Borhan Zoufan,**  
CTO, Caspian IT Group, on the rationale  
for choosing Acronis Cyber Cloud



# Summary

The history of tech advancement is one of consolidation. Last century's costly, dishwasher-sized pile of networking gear (router, switch, remote access server, digital modem) has shrunken to one cheap, compact, easy-to-manage box. Your dad's old voice - and text-only "feature phone" - has been supplanted by an iOS or Android device loaded with 60 applications.

The march toward integration is inevitable, with benefits to suppliers and customers alike. That same progression has arrived in the MSP world in the form of the **Five Levels of MSP Platform Integration**, allowing you to:



**Land new customers**, grow existing accounts, reduce churn and fatten margins



**Lower your customers' business risk** with greater cybersecurity, protection against data losses, and reduced downtime



**Reduce the heterogeneity of your service delivery infrastructure**, minimize your integration challenges, and lower your overall vendor and technology management costs



**Take advantage of AI**, customer self-service, and other automation technologies to achieve better business and operational results with lower infrastructure and personnel costs

## For more information

**Learn how you can take advantage of the Five Levels of MSP Platform Integration in your own business:**

Discover more information in the [Acronis Resource Center](#)

READ ON

Get a complimentary 30-day trial of [Acronis Cyber Backup Cloud](#)

TRY NOW

Reach out to [Acronis](#) directly

REQUEST DEMO

**Acronis**

Learn more at  
[www.acronis.com](http://www.acronis.com)

Copyright © 2002-2020 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2020-03