SMALL BIZ THOUGHTS
by Karl W. Palachuk

THE FAST TRACK TO BETTER IT OPS, HELP DESK AND MSP TEAM PRODUCTIVITY

E-book commissioned by Acronis

CONTENTS

The Fast Track to Better IT Ops, Help Desk and MSP Team Productivity 3

All Hail the API — The Good, the Bad, and the Ugly.. 4

The True Cost of Tool Sprawl... 5

Welcome to the Well-Integrated Solution... 6

Company Maturity Matters.. 8

Invest in the Stack.. 9

Summary Conclusion.. 10

References..11

Additional Resources..12

THE FAST TRACK TO BETTER IT OPS, HELP DESK AND MSP TEAM PRODUCTIVITY

By Karl W. Palachuk

In December 2019, Boeing launched its Starliner spacecraft on a mission to meet up with the International Space Station. The mission was straight-forward: successfully launch the vehicle; dock with the International Space Station; return safely to Earth.

Fifty-five minutes after launch, NASA reported that Starliner experienced an "off-nominal insertion." That's the techno-babble way of saying the spacecraft was in the wrong orbit.

They missed the International Space Station. They missed! Luckily, the spacecraft was a crewless test flight.

In a world of absolute precision, how was this "miss" possible? Very simply, two different software systems did not communicate perfectly with one another. While there was every intention to provide perfect, open communications, there was still a glitch: an onboard clock was set to the wrong time, so the spacecraft wasn't where it was supposed to be when it was supposed to be there.

Stop and think about that: NASA, SpaceX, and Boeing have all pledged to work together in an environment of cooperation and openness. All partners are well-intentioned and focused on the same set of goals. Everyone is facing the same direction and seeking the same outcome.

In all, Boeing spent $1.5 billion to get it right. And they missed.

There's a lesson here about the relationship between complexity, interconnections, and the efficient use of software. Even when partners agree on design specifications and build on completely open, well-documented platforms, things can still go wrong.

Now imagine an environment in which the developers are not partners but competitors. Each publishes specifications on how to connect through their application programming interface (API), but they do not communicate directly with one another.

The result is exactly what you would expect: more complicated, less streamlined, and more prone to problems.

ALL HAIL THE API — THE GOOD, THE BAD, AND THE UGLY

Technology always moves fast. While other industries enjoy a new generation of business every decade, IT sees a new generation of technology every 18 to 24 months. If your operation hasn't changed in five years, you know you're behind the times.

As we leave 2020 behind and move into 2021, we're in an era dominated by APIs, which emerged in the early 2000s as a way to help applications work together, exchange information, and automate processes.

APIs were a great addition to many managed service providers as they allowed a variety of tools to work together. Of course, the more API middleware you bought, the higher your cost is to deliver services. Sometimes that middleware was rather expensive and, more often than not, it was a kludge — but it worked!

What was once a wonderful new strategy had become a "build your own Frankenstein's monster" construction kit.

Skip ahead to today. APIs are very mature. But, even under the best of circumstances with the best programming, you still need to manage API connections. When you're connecting software from two different companies, a change on either side can "break" functionalities. If you have a third-party connection between the two, it's even more complicated.

Every connection requires some minimum level of management. And every connection represents a potential security hole that has to be monitored. Ransomware is now big business, and cybercriminals have discovered that IT service providers are rich sources for stealing data and spreading code. As with all attacks, they can pick any entry point they wish and pound against it — which means you have to defend every possible attack point.

The dirty little secret of all software development is that maintenance and support always end up costing more than the software itself. (As IT service providers, we know this because we make a living providing some of that support.) On top of this, each set of connections increases the need for monitoring, maintenance, and support.

THE TRUE COST OF TOOL SPRAWL

In addition to paying a variety of vendors for a variety of tools, "tool sprawl" leads to increased costs for training, integration, and maintenance. One Gartner study pointed out that tool complexity leads to increased expenses on multiple fronts. In the end, the "ugly" part about APIs is that while they connect various software, they do so inefficiently. Each connection adds complexity, documentation, training, and two or more additional connections that have to be maintained.

The effort that goes into maintaining a complex, interconnected system also represents a direct hit to overall productivity. Every hour spent maintaining your systems is an hour that's not spent helping end users.

In one recent study, Forrester Research found that reliance on legacy toolsets was a major barrier to modernization and digital transformation. They found that 86% of companies use at least one legacy tool, and only 12% use fully integrated, modern monitoring tools.

This reliance on a variety of outdated and poorly-connected tools results in higher costs to support the environment, degradation in service delivery, and increased security risks (more on this below). Another frustrating cost of using multiple tools is integration. Almost half (46%) of companies reported that they "spend too much time and money maintaining and integrating the varied security protocols of every tool."

On top of all that, multiple tools result in overlapping functions. In other words, you are paying for the same functionality two or three times. In each case, at least one tool is not using all of its integrated functions because it's using a similar function from another tool. These overlapping functions mean most tools are underutilized due to complexity, lack of resources, and the burden associated with managing multiple tools.

> In summary, most companies are using a variety of tools that are not well-connected by design. They are spending money on tools with duplicate functions, which increases maintenance costs as well as up-front license fees. The operation requires more training, more monitoring, and more documentation with each product added to the toolset.
>
> But it doesn't have to be that way.

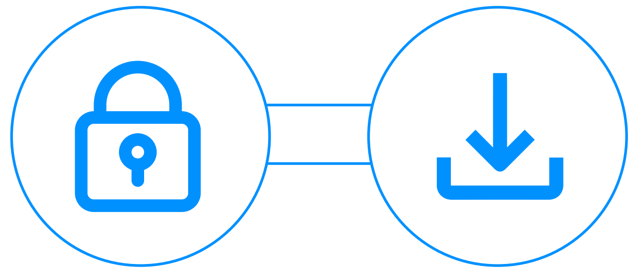
WELCOME TO THE WELL-INTEGRATED SOLUTION

We've come a long way from the early, clunky, APIs. Increasingly, IT teams are choosing software options that are integrated by design rather than patched together after the fact. We're moving away from the world dominated by API translations.

Complexity is an important factor in software development and maintenance. Just as you would expect, complexity leads to increased costs for maintenance, security, and support labor. When you have separate systems for backup,

Example One

With two software solutions and one connector, you might have one, two, or three different partners who need to work together. Any one of them could make a change that either "breaks" the connection or creates a vulnerability that could be exploited.



Example Two

With three software solutions and two connectors, you might have one, two, three, four, or five different partners who need to work together. Again, any one of them could make a change that either breaks the connection or creates a vulnerability that could be exploited.

Example Three

Now let's look at the emerging "integrated" world of security applications. These are applications designed to work together from the start. They're all built by the same team. They work together by design.

malware protection, remote desktop support, and management, you also have lots of connections — and each connection represents several pain points and possible threat vectors within your environment. Here's what I mean.

Let's say you want to connect two applications and their services, such as backup and antivirus. There are several variations of what this might look like. Are they built by the same company? Are they designed to work together from the start? If there's a connection between the two systems, was it written by one of the primary companies or a third party?

As software complexity is reduced, you enjoy the benefits of greater efficiency, lower maintenance, increased productivity, and greater security. You also achieve lower costs from the start since you're not paying for third-party middleware to make your application stack work together, or the additional administrative time needed to manage additional applications.

There's a growing problem among IT service providers called vendor fatigue — that simply means too many invoices from too many companies as a result of making your systems work the way they're supposed to.

One company has addressed this problem head-on. Acronis has built a stack of products that work seamlessly with one another. Designed from the bottom up, Acronis Cyber Protect maximizes efficiency by reducing complexity and lowering the total cost of ownership (TCO). Says Lauren Beliveau, an Acronis Product Marketing Manager, "We don't just have a bunch of products — we have a stack of solutions."

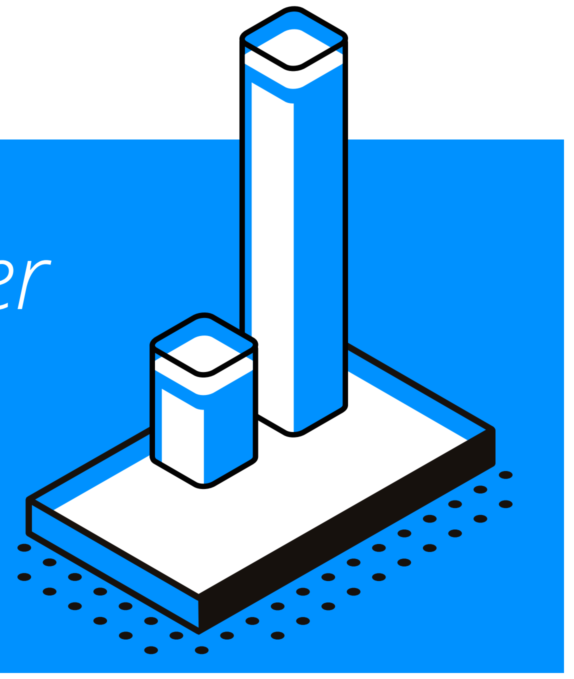
This is not just a theoretical problem. In the world of security, the old "patchwork" of legacy tools represents a serious threat that requires additional monitoring. Every connection represents a potential vulnerability: But so does every patch and update. Not only do you need to apply patches: you then must monitor things to make sure you haven't introduced a problem. Sometimes, you need to unpatch and repatch as vulnerabilities emerge.

Unfortunately, one common approach to patching is to wait for a period of time to apply patches to verify that they will not introduce additional problems, incompatibilities, or weaknesses. This practice leaves the applications open to known vulnerabilities for an extended period of time.

On top of that, poorly-integrated applications from different vendors may not share data, alerts, automation, documentation, user interfaces, agents, and more. Every weakness in a connection is a weakness in security. Today, the cost of this weakness is too great to be ignored.

With Acronis Cyber Protect, the antivirus knows there's a backup and scans it. With a completely integrated solution, tools such as backup and antivirus work more efficiently together. Backups are automatically scanned for threats such as viruses, malware, and ransomware to ensure that the data is clean. Patches are applied to backups as well as live systems. All of this is seamless. Literally.

Reduced software complexity means greater efficiency, lower maintenance, increased productivity, and greater security



COMPANY MATURITY MATTERS

Another factor that's seldom considered is the maturity of the company that makes the tools. As companies grow from startup to fully mature, they go through several stages. In the beginning, they have an immature product that does one thing (e.g., antivirus). Over time, the product becomes fully functional. As the company moves from startup to established, it focuses on getting its product into the market, and maybe even making money.

Established startups focus on increasing features and connectivity. Thus, they embrace the all-powerful API. Their goal at this stage is to connect with everyone. This stage is perhaps the most kludgy. It works, most of the time, but the APIs are not mature and everything changes all the time. If they're successful, users now demand more features — so they move to the next stage: widening their base.

Companies focused on widening their base are also focused on buying or building new features. Their strategy at this stage is to obtain clients by offering more functionality and working with more competitors. The ultimate vision is to grab market share by responding to user demands and doing more with their toolset. This expansion stage is also a time of great internal changes and constantly trying to keep up with evolving APIs — internally, between the products they're buying and integrating, and between their products and their competitors.

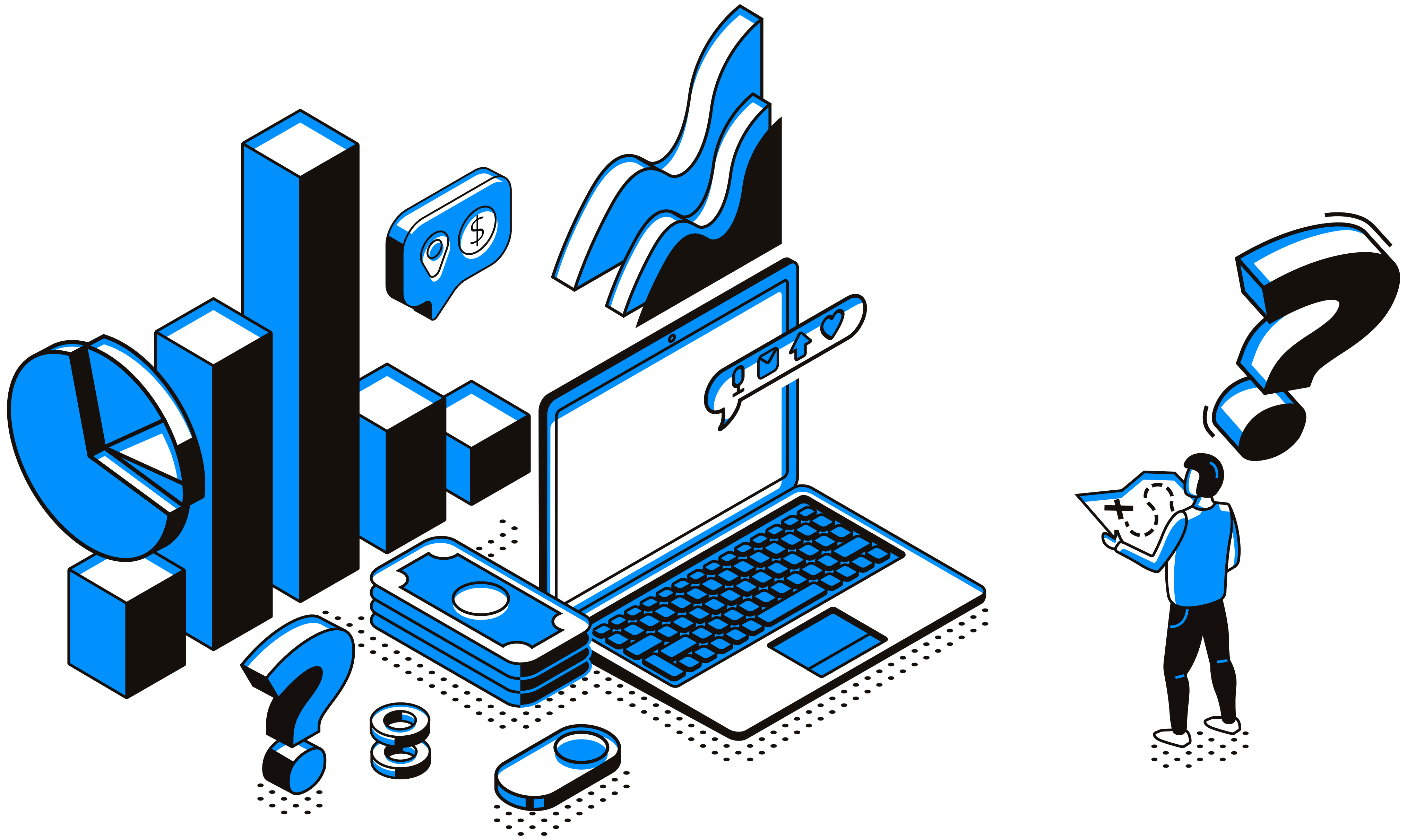
The next stage is financial expansion. Whether it's through venture capital or some other funding source, there's a point when companies need money to expand. That, in turn, leads to a reduction in customer responsiveness. As more of the management focus moves from functionality to finance, sales become more important than fixing problems or adding features.

You've seen this in mergers over the years: a super responsive vendor suddenly stops fixing things and the product roadmap becomes very unclear to the IT professionals who rely on the software. At this stage, sales is the sole focus of activity within the company. Development (including fixing things) is reduced significantly.

Only a few companies live long enough to become truly mature, developing well-integrated tools that work seamlessly together, and with enough support on the programming side to add new features without breaking anything or creating new problems. In addition to the technical challenges, mature companies have settled into a long-term pattern of funding ongoing development as well as sales and customer support.

As technology changes faster and faster each year, new functionality is required to address new challenges. This fact applies to cybersecurity more than any other area. Ten years ago, viruses were annoying and destructive. Today, they can cost millions of dollars in ransom on top of the cost of downtime.

Less mature companies and those side-tracked by mergers and acquisitions are stuck with older products. Very often, they don't have the time, money, or internal focus to keep up-to-date with the demands of the evolving security environment.



At best, they have old solutions. At worst, their solutions do not integrate with newer tools.

As the complexity of your toolset goes up, the efficiency goes down. In addition to addressing the problem of multiple APIs, you have to manage the inner-activity of software at various levels of maturity, support by companies at various levels of maturity of their APIs, and documentation.

You want to build a great stack. Sometimes that means looking for the "best in class" options, even if they're from different vendors. Whenever possible, you buy deeply into a single stack in order to increase efficiency, security, and profit.

> Now, with Acronis Cyber Protect, you have the best of both worlds. Acronis is widely recognized as the leader in data protection and recovery. They've built an entire collection of world-class solutions to protect data, applications, and systems and eliminate the troublesome middleware.
>
> Acronis Cyber Protect includes features the competition will be scrambling to copy, including applying patches to backup images so that restore procedures cannot roll back the security level of client machines.

With ransomware, multi-million-dollar lawsuits, and government regulations, the 2020s are not the time to waste money and effort building a collection of security tools that you hope work well together. You need solutions that provide cutting-edge functionality and security while reducing complexity, maintenance, and the costs that go with them.

Step up to the only security stack built by design to be fully integrated.

SUMMARY CONCLUSION

> *“With Acronis Cyber Protect, we literally have one solution that does everything 10 other solutions do separately.”*

Jason Menezes,
Department Head of Backup
and Disaster Recovery at Datategra

Security can no longer be considered a bolt-on feature to other services. In the 2020s, technology consultants have to have rock-solid, total solutions that provide unparalleled security while letting the users go about their business.

Complexity decreases efficiency and productivity while increasing costs for maintenance, documentation, and training. The more “parts” you have, the more connectors you have. A completely integrated stack, built to work seamlessly by design, maximizes overall security while reducing complexity and all the costs that go with it.

APIs will still be around for a long time. Thankfully, you can be productive managing complex, interconnected systems once you move to the totally integrated stack from Acronis, the leader in cybersecurity and data protection.

Connections are good. Integration by design is better.

REFERENCES

https://www.msn.com/en-us/news/technology/boeings-software-troubles-show-an-engineering-culture-clash/ar-BB16xEdq

https://www.forbes.com/sites/jonathanocallaghan/2019/12/20/boeing-starliner-spacecraft-launches-to-the-international-space-station-heralding-a-new-era-for-american-human-spaceflight/

If This Then That
https://ifttt.com/

Zapier
https://zapier.com/

Programmable Web
https://www.programmableweb.com/

Salesforce.com
www.salesforce.com

Harvard Business Review, "The Strategic Value of APIs."
https://hbr.org/2015/01/the-strategic-value-of-apis

"Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices."
https://www.gartner.com/en/newsroom/press-releases/2016-07-19-gartner-says-organizations-can-cut-software-costs-by-30-percent-using-three-best-practices

Forrester Research, "Prevalence Of Legacy Tools Paralyzes Enterprises' Ability To Innovate."
https://sciencelogic.com/wp-content/uploads/sciencelogic-os.pdf

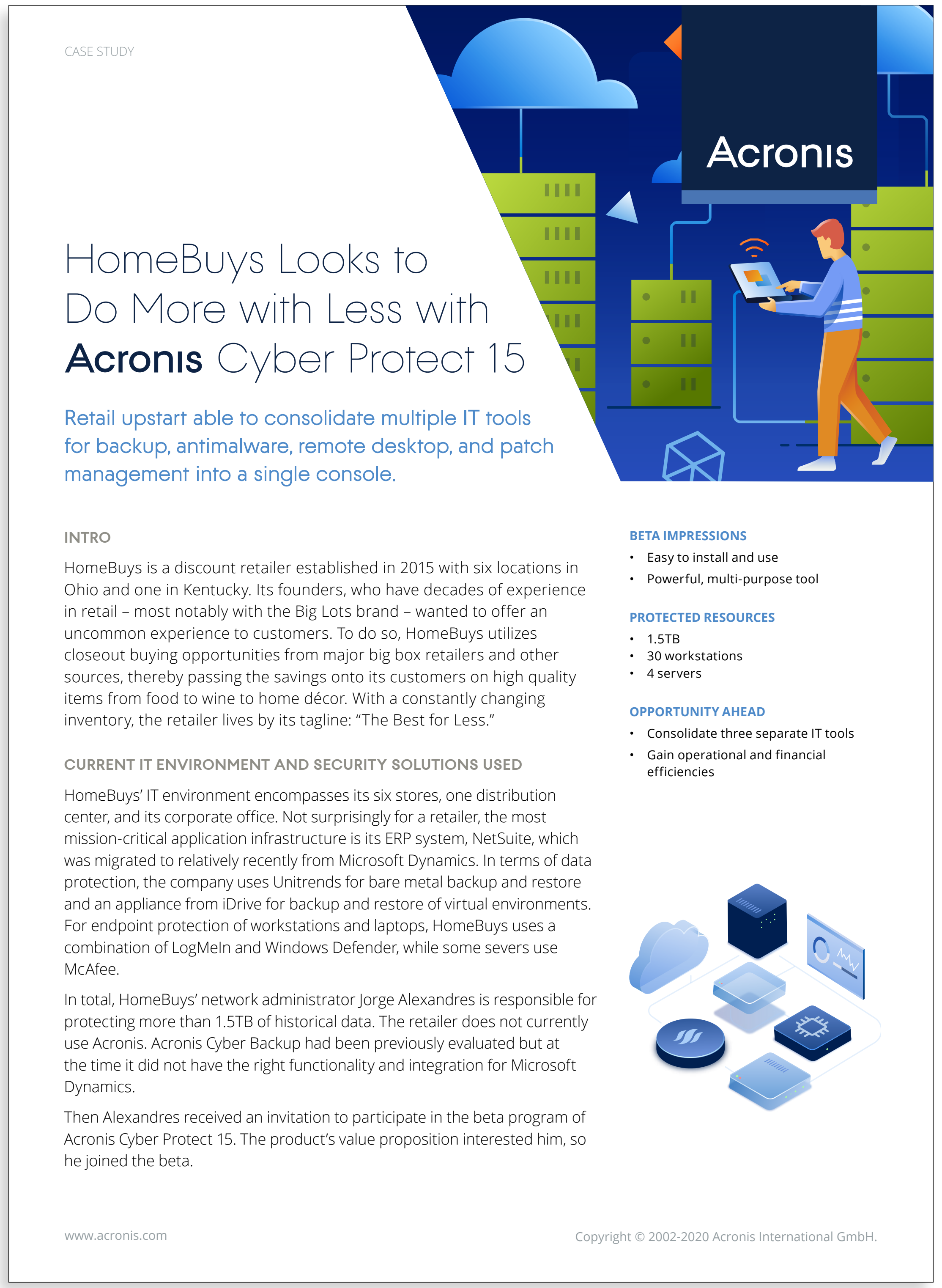
"Struggling With Toolchain Sprawl? You're Not Alone."
https://dzone.com/articles/toolchain-sprawl-youre-not-alone

ABOUT THE AUTHOR

Karl W. Palachuk has built and sold two managed service businesses in Sacramento, CA. He is the founder and president of the Sacramento SMB IT Professionals Group, and author of several books, including The Network Documentation Workbook and Managed Services in a Month.

Karl has been a featured speaker at conferences and seminars all over the world for more than 15 years. He is a Microsoft Certified Systems Engineer with a Bachelor's Degree from Gonzaga University and a Master's Degree from The University of Michigan. He is also a Microsoft Small Business Specialist, and is an original member of Microsoft's Small Business Specialist Advisory Panel.

ADDITIONAL RESOURCES



CASE STUDY

HomeBuys Looks to Do More with Less with Acronis Cyber Protect 15

Retail upstart able to consolidate multiple IT tools for backup, antimalware, remote desktop, and patch management into a single console.

INTRO

HomeBuys is a discount retailer established in 2015 with six locations in Ohio and one in Kentucky. Its founders, who have decades of experience in retail – most notably with the Big Lots brand – wanted to offer an uncommon experience to customers. To do so, HomeBuys utilizes closeout buying opportunities from major big box retailers and other sources, thereby passing the savings onto its customers on high quality items from food to wine to home décor. With a constantly changing inventory, the retailer lives by its tagline: "The Best for Less."

CURRENT IT ENVIRONMENT AND SECURITY SOLUTIONS USED

HomeBuys' IT environment encompasses its six stores, one distribution center, and its corporate office. Not surprisingly for a retailer, the most mission-critical application infrastructure is its ERP system, NetSuite, which was migrated to relatively recently from Microsoft Dynamics. In terms of data protection, the company uses Unitrends for bare metal backup and restore and an appliance from iDrive for backup and restore of virtual environments. For endpoint protection of workstations and laptops, HomeBuys uses a combination of LogMeIn and Windows Defender, while some severs use McAfee.

In total, HomeBuys' network administrator Jorge Alexandres is responsible for protecting more than 1.5TB of historical data. The retailer does not currently use Acronis. Acronis Cyber Backup had been previously evaluated but at the time it did not have the right functionality and integration for Microsoft Dynamics.

Then Alexandres received an invitation to participate in the beta program of Acronis Cyber Protect 15. The product's value proposition interested him, so he joined the beta.

BETA IMPRESSIONS

- Easy to install and use
- Powerful, multi-purpose tool

PROTECTED RESOURCES

- 1.5TB
- 30 workstations
- 4 servers

OPPORTUNITY AHEAD

- Consolidate three separate IT tools
- Gain operational and financial efficiencies

www.acronis.com

Copyright © 2002-2020 Acronis International GmbH.

Acronis Blog: Provides the latest updates and insights from the world's cyber protection leader.

Acronis YouTube Channel: Delivers frequent videos of use cases, demos, cyberthreat analysis, and company news.

Acronis Resource Center: The go-to hub for cyber protection white papers, e-books, in-depth articles, tutorials, infographics, etc.

Acronis Events: Ongoing series of events, webinars, interviews, etc., including details on joining.

ABOUT ACRONIS

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions. With award-winning AI-based antimalware and blockchain-based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on-premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,500 employees in 33 locations in 18 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages.

Small Biz Thoughts
by Karl W. Palachuk

SmallBizThoughts.com

E-book commissioned by Acronis

acronis.com