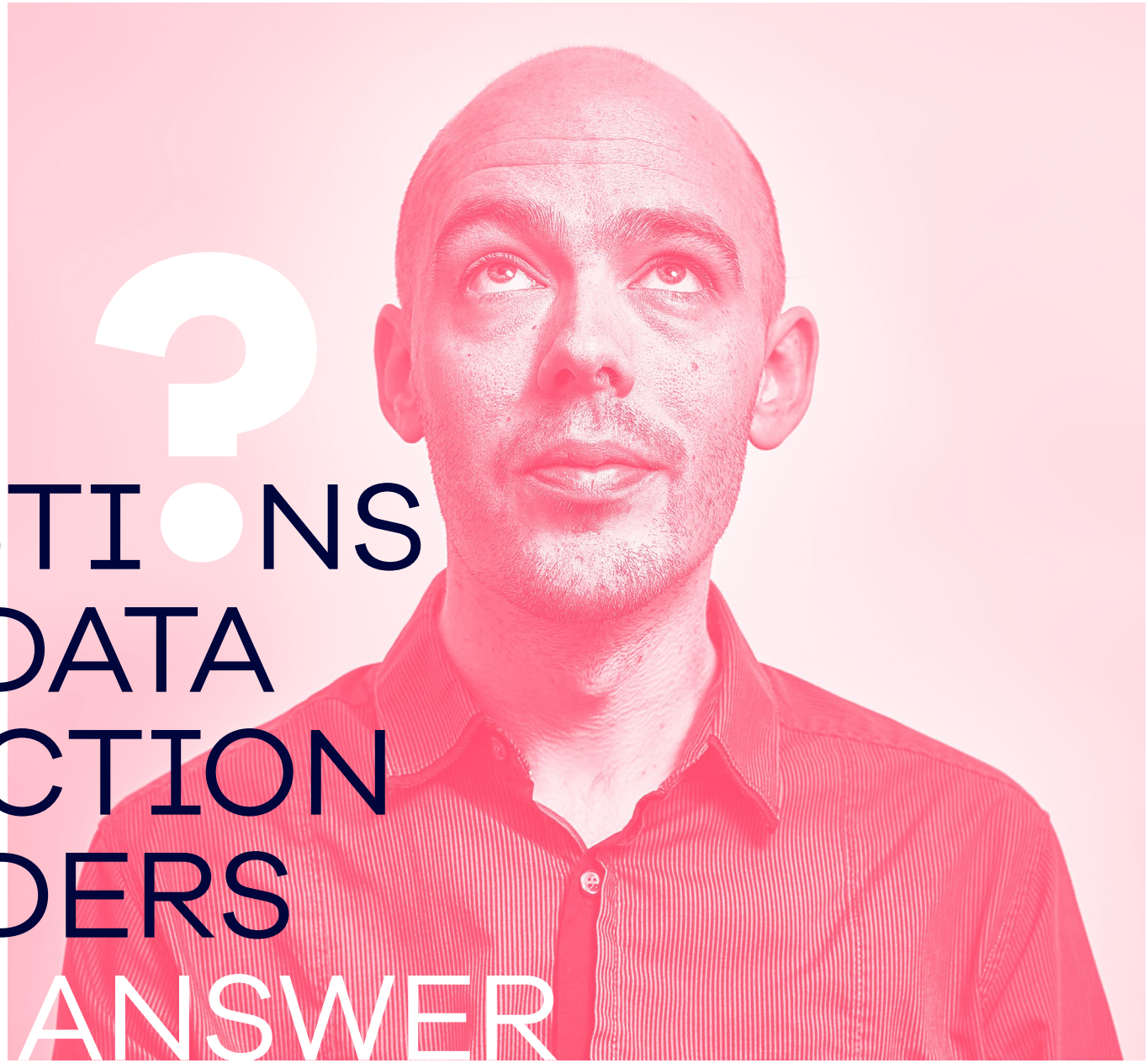


5 QUESTIONS MOST DATA PROTECTION PROVIDERS WON'T ANSWER

Commvault®

eBOOK

CONTENTS

OK, LET'S START WITH THE OBVIOUS.

Data is **gold**, but only if you can use it.

If you've gone to the trouble of downloading this eBook, you already understand the critical importance of cyber resilience. It's everything to the success of your enterprise.

Data is also everywhere in private and public clouds, in SaaS, on-prem, at the edge, and spread across your organization.

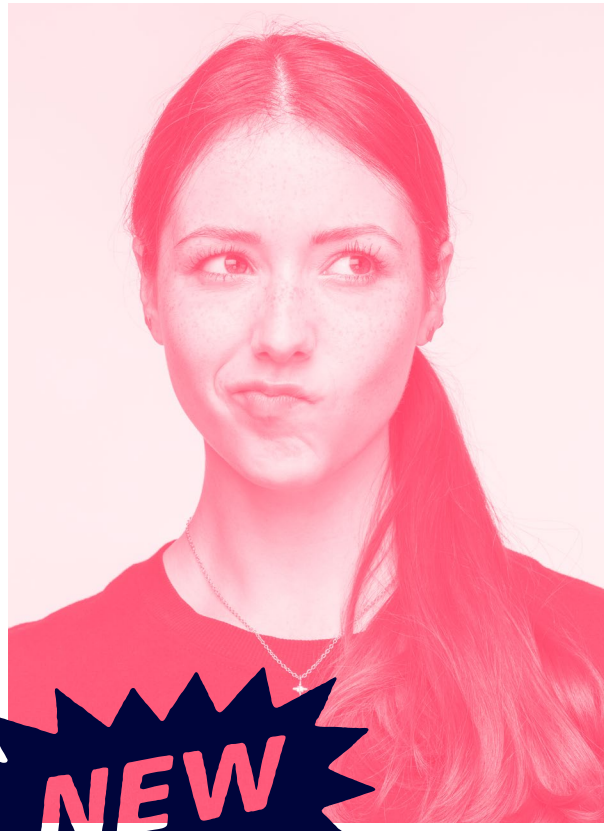
Which makes your choice of cyber resilience platforms equally critical.

Of course, most vendors will tell you exactly what you want to hear: that all your data is covered, protected, and ready to be restored. Making it hard to tell one from the next.

That's why we've put together this eBook to arm you with the right questions to ask when evaluating any data protection vendor, even the one you have now. Time is money, so let's dive in.

Question it:

IS MY CLOUD DATA PROTECTED?



Having more and more workloads in the cloud offers the durability you need to ensure that your data and applications are always available. But what about data corruption, malware, or other related incidents that could leave you with highly resilient "bad data"?

The first mistake many companies make is to assume that cloud providers are responsible for data protection. But if you ask, most cloud providers have a shared responsibility model, where the users are responsible for protecting their data. Yes, some cloud/SaaS native offerings provide their own native data protection tools. But others, like Microsoft's M365, advise investing in a third-party solution like Commvault to ensure enhanced ransomware protection and multi-cloud protection.

Another common misconception is that cloud-delivered workloads, such as those provided by Azure, AWS, and OCI are either too new or different for traditional data protection practices. Or that data protection only covers where the data was in the past, not where it is moving to in the future.

That's the old way of thinking. Commvault® Cloud, powered by Metallic® AI is the only cyber resilience platform built to meet the demands of the hybrid enterprise.

90% of organizations could not recover **100%** of data they backed up in a public cloud service.

ESG

THE BOTTOM LINE

Cyber resilience is critical for cloud native and SaaS-based applications. Modern companies need extended retention, isolated cyber protection, rapid and full-fidelity recovery controls.

Question it:

IS MY CLOUD DATA PROTECTED?

"WE LOOKED AT BARRACUDA AND VEEAM, BUT **METALLIC® OFFICE 365 BACKUP** IS THE ONLY SAAS SOLUTION THAT GIVES US THE PERFORMANCE AND SCALABILITY WE REQUIRE TO PROTECT OUR CRITICAL OFFICE 365 ENVIRONMENT."

Fadi Alzebdeh, Manager, IT – Operations, Juma Al Majid

"IT'S CLEAR TO ME THAT COMMVAULT AND MICROSOFT ARE **COMMITTED TO BUILDING INCREASINGLY INTEGRATED SOLUTIONS** THAT MEET THE SCALE AND SCOPE OF MY ORGANIZATION'S NEEDS AND REQUIREMENTS IN A HYBRID WORLD."

Johns Hopkins University

5X BETTER TCO

vs. Cloud-Native
Data Protection Tools

12 OUT OF 12 LEADER

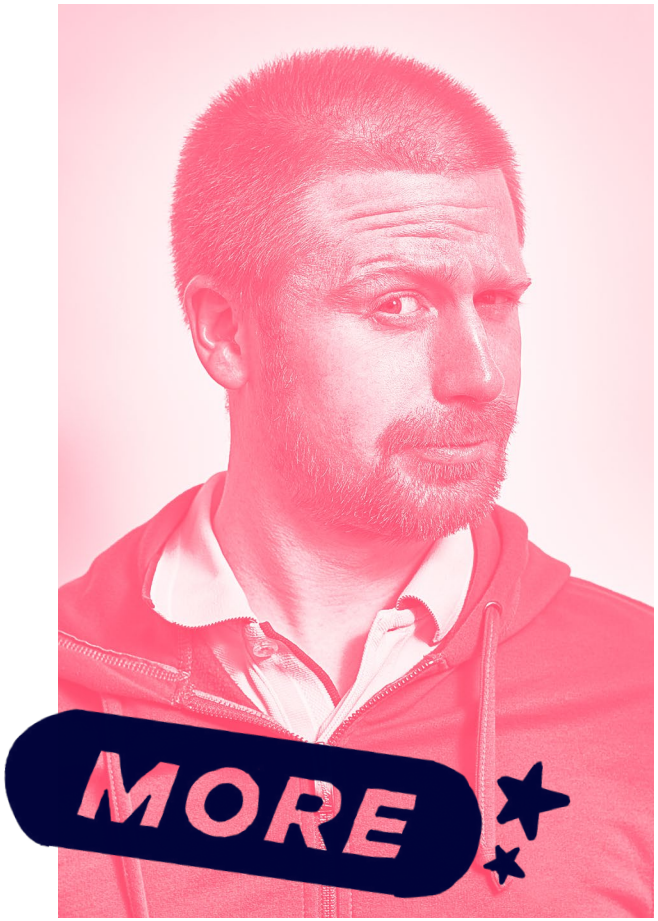
of Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions every year

FIRST FULLY MANAGED DPaaS

to support multiple clouds

Question it:

WILL MORE BOLT-ON BACKUP TOOLS MAKE US MORE SECURE?



When it comes to data security, there is a belt-and-suspenders mentality, where more is always better. But more tools mean more infrastructure and more costs, which ultimately leave more security gaps for bad actors to exploit by reducing visibility and creating inconsistent management and mobility. Not to mention the increased cost of staffing and training to master the complexities caused by multiple tools, appliances, and interfaces.

Truth is, a modern cyber resilience platform, like Commvault, should be capable of protecting and securing your data and applications, including cloud-native (DBaaS, PaaS, IaaS), Kubernetes, and SaaS without adding extra tools or vendors.

More tools = more risk.

That just seems like common sense, right? But when you start asking questions, you find that vendors like Veeam, Veritas, and others all need multiple products to protect your entire data environment. One tool for your traditional workloads, one for cloud-native, another for SaaS, and a special one for Kubernetes. Layers and layers of complexity that, in some ways, only make things worse.

And that's not the least of it. Yep, you still need to add in security and ransomware detection. Veeam boasts about "immutability everywhere," but the truth is the opposite. Even for basic backup immutability, Veeam still mainly relies on third-party storage solutions. Dell also lacks any ransomware detection until you pony up for expensive tools and infrastructure from another vendor. So read those specs closely.

THE BOTTOM LINE

These are just a few common examples of this bolt-on approach to data protection. Accumulating more layers only weakens your defenses. So, make sure your cyber resilience is truly seamless.

Question it:

WILL MORE BOLT-ON BACKUP TOOLS MAKE US MORE SECURE?

"WE CONSIDERED OTHER SOLUTIONS, INCLUDING VEEAM, BUT **COMMVAULT IS THE ONLY SOLUTION** THAT COULD RELIABLY SUPPORT A WIDE RANGE OF TECHNOLOGIES."

Sebastian Kober, IT-Leiter, Leipziger Messe GmbH

1>6

syncreon saved $500K by consolidating six backup solutions into one.

"**WITH COMMVAULT, IT'S JUST ONE PLATFORM.** I DON'T HAVE TO GO TO A DIFFERENT INTERFACE TO MANAGE STORAGE, SCHEDULES, OR SECURITIES. REMOVING THAT COMPLEXITY BRINGS A WHOLE LOT OF COST REDUCTION FOR US."

Robert Welsford, IT Manager, Morrison Hershfield

Question it:

WILL YOUR DATA PROTECTION COVER ALL YOUR WORKLOADS?

Any vendor that says broad coverage of workloads is "complex" is missing the point. We live in a multi-cloud world where many enterprises use different clouds and platforms based on their workloads. In a recent study, 53% of respondents said their IT environment was more complex than it was two years ago and that trend shows no sign of slowing down.*

If it doesn't protect everything, are you really protected? Broad workload coverage that ensures no data is left exposed and unprotected is absolutely essential. More than that, companies need cyber resilience platforms that go beyond traditional backup and recovery to protect against evolving threats of tomorrow—reducing their risk and ultimately controlling their costs.

"Complexity" demystified. So, when a vendor labels any product with the capability to cover any workload as "complex," what do they mean? Usually, it's that they have limited capabilities and will try to sell customers separate point solutions, which add cost, risk, and, ironically, complexity.

THE BOTTOM LINE

The answer you really want to hear is, "Your workloads are covered, and with one solution." But you won't hear that from Cohesity. Their protection is limited in terms of what data they can backup, lacking support for critical workloads like Azure Active Directory, Oracle Cloud, and many other cloud-native databases and applications. You can't mix/match different appliance models or vendors together in a cluster.

You'll hear the same thing from Rubrik, who suffers from some of the same limitations as Cohesity as far as cloud workloads, databases, and applications.

Commvault

* ESG research (From Data Backup to Data Intelligence, January 2022)

Question it:

WILL YOUR DATA PROTECTION COVER ALL YOUR WORKLOADS?

"WE WERE LOOKING FOR AN OFFERING THAT COULD PROTECT THE MANY KEY PLATFORMS DEPLOYED ACROSS OUR ENVIRONMENT, AND COHESITY COULDN'T CHECK EITHER OF THOSE BOXES. **COMMVAULT'S MODERN APPROACH TO DATA MANAGEMENT** WAS ABLE TO DELIVER ON BOTH PLUS PROVIDE THE RECOVERY SPEED DEMANDED BY OUR CUSTOMERS – IN TODAY'S FAST-MOVING CULTURE, NO ONE WANTS TO WAIT. THEY WANT THEIR DATA FAST AND THEY WANT TO BE ABLE TO USE IT AND CONSUME IT AS QUICKLY AS POSSIBLE. THAT'S DEFINITELY ONE OF THE MAJOR MOTIVATORS WE HAD FOR CHOOSING COMMVAULT."

Gilman Treantos, Administrator, IT – Backup/Storage,
Blue Cross & Blue Shield of South Carolina

50% LOWER TCO

for Hana TI, a financial IT service provider, with Commvault Complete Data Protection

https://www.commvault.com/resources/case-study-hana-ti

TOTAL RESILIENCE

"COMMVAULT SUPPORTS ALL TYPES OF WORKLOADS; **IT IS LITERALLY UNIVERSAL**. METALLIC RUNS IN THE CLOUD, BUT COMMVAULT HAS NOT FORGOTTEN THE IMPORTANCE OF PROTECTING ON-PREM WORKLOADS."

ESG research (From Data Backup to Data Intelligence, January 2022)

Question it:

WHAT DO YOU MEAN WHEN YOU SAY "ZERO TRUST"?

Zero trust is a cybersecurity model that withholds permission to access a network, application, or data unless and until the user's identity, device, location and their related security posture can be verified. Never trust, always verify. It's not a product, but a strategy, and to do it right requires diligence and coordination across multiple teams and technologies.

So, it's a bit odd that some data protection vendors, like Rubrik, claim to be the ONLY zero trust security platform. You might ask what that means. Not only that, but their ransomware features are reactive and not built in – they live outside your environment and only activate after the damage is done. Which means their tools could become cut off from the very systems they are intended to protect. Talk about zero trust.

Of course, zero trust is only one part of modern security. It's great for protecting the perimeter, like a home security setup with cameras, locks, window sensors, and a fence. But once you welcome someone in, they have free reign to access your possessions.

A more comprehensive security solution, like Commvault Cloud, combines zero trust with fully integrated proactive threat deception technology that actively tracks intruders and leads them away from valuable data.

THE BOTTOM LINE

Insurance and warranties don't matter if you can't recover your data. Don't waste time filing a claim when you can just recover your data.

Question it:

WHAT DO YOU MEAN WHEN YOU SAY "ZERO TRUST"?

AIR-GAPPED

immutable storage in the cloud.

Using Commvault Cloud Air Gap Protect™, you can easily house data in a secure, air-gapped cloud storage target.

Commvault Cloud is currently

THE ONLY

FedRAMP-Ready High Certified SaaS Data Protection Solution.

Question it:

IS DATA SECURITY BETTER THAN DATA PROTECTION?

Admittedly, it's a bit of a trick question, but one worth asking. The truth is that data security is vitally important and essential. But it's also just one element of true cyber resilience.

So, beware. That's an outdated view of the world. Cyber resilience looks very different.

It's still backup, but also data security, defense, recovery, automation, and other elements. Really, everything businesses need to insulate themselves from a new wave of threats.

If you look beyond the hype, you'll quickly see that the capabilities some competitors claim as unique – immutability, zero trust, backup monitoring – are actually just table stakes in a robust data protection solution. And an unhelpful distraction from a less-than-complete recovery solution.

THE BOTTOM LINE

Security is a subset of cyber resilience. Cohesity, for example, offers only reactive threat detection, and it's limited to looking at their backup data. By the time a threat has been detected, the damage has been done.

Veeam also talks a big game, but their data security appears to be an afterthought. It lacks many key features needed to harden security, like enterprise-wide ransomware and malware detection or even multi-person authentication, to prevent issues from rogue admins.

When it comes to backup, Veeam has no way to automatically restore the last good copy of your data, leaving you to manually comb your backups. They might boast about "immutability everywhere," but the truth is the opposite. Hence, their reliance on third-party storage solutions to provide that functionality.

Question it:

IS DATA SECURITY BETTER THAN DATA PROTECTION?

"OUR EXISTING BACKUP PRODUCTS WERE NOT MEETING OUR NEEDS. VERITAS HAD DAILY ISSUES AND OUR BACKUPS WERE JUST NOT RELIABLE. ANY RESTORE REQUESTS THAT CAME IN, WE JUST CROSSED OUR FINGERS AND MADE A BEST EFFORT AT RECOVERY. VEEAM DID MUCH BETTER WITH OUR VIRTUAL ENVIRONMENT, BUT LACKED THE ABILITY TO BE A FULL ENTERPRISE SOLUTION FOR OUR PHYSICAL SERVERS AND APPLICATIONS. COMMVAULT TO THE RESCUE! **OUR LONG-STANDING BACKUP AND RESTORE PROBLEMS ARE NOW A THING OF THE PAST**."

Woodward Inc.

66% LOWER BACKUP COSTS

"METALLIC CUT OUR BACKUP COSTS BY **TWO-THIRDS**."

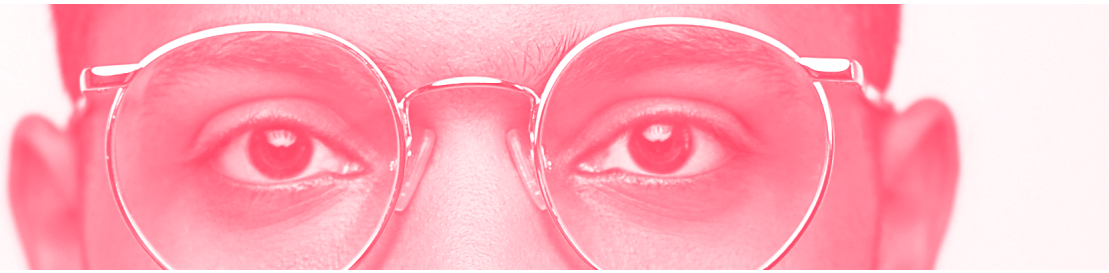
Economic Benefits of Commvault with Metallic on Microsoft Azure

15X REDUCTION IN MANAGEMENT

"MULTIPLE COMPANIES THAT FOUND 15+ DIFFERENT BACKUP SOLUTIONS RUNNING, ALL OF - WHICH WERE **ULTIMATELY REPLACED BY METALLIC**."

TechTarget Enterprise Strategy Group, 2023

WHAT TO LOOK FOR



Now that you have the questions, here are a few of the answers you really want to hear.

Q "WE COVER ALL WORKLOADS TO ELIMINATE GAPS IN DATA PROTECTION AND MONITORING."

A Commvault supports the broadest spectrum of data platforms, workloads, and cloud-native applications. Giving you the peace of mind that comes with knowing that, whatever and wherever your data lives, Commvault delivers consistent and integrated protection.

Q "OUR SECURITY IS BUILT-IN AND PROVIDES EARLY WARNING OF POTENTIAL THREATS TO PRODUCTION DATA."

A Commvault's core data security features are engineered right into our code and not reliant on any third-party apps. It's a layered approach to threat detection that looks beyond your backups to actively monitor live data. So, you get earlier warnings of potential threats and the ability to quickly respond and mitigate any impact.

Q "YOU HAVE THE FLEXIBILITY TO CONTROL YOUR COVERAGE AND LOWER TCO."

A With Commvault Cloud, you can build and scale your environment with a mix of appliance, reference architecture, virtual, cloud, and even SaaS to best fit your evolving business needs. But features like global deduplication, dynamic provisioning, and power management help you reduce your infrastructure costs on-premises and in the cloud. **We're the only company that can do this.**

TRY COMMVAULT FOR FREE TODAY >

COMMVAULT IS CYBER RESILIENCE.

For the most workloads at more than 100,000 organizations and 3.8 Exabytes of cloud data at the lowest TCO.

"COMPARED TO OTHER PRODUCTS LIKE DELL EMC AND VEEAM, COMMVAULT OFFERS THE MOST COMPLETE SOLUTION. **THIS SAVED US $150,000 IN TCO**."

Adrian Lerch, System Engineer at BGC

Learn how BGC consolidated from multiple backup products to a single solution >

"**THE INTEGRATION WITH COMMVAULT WAS HASSLE-FREE**. WE CAN NOW LEVERAGE MORE FEATURES TO SIMPLIFY DATA MANAGEMENT AND ENSURE DATA SECURITY."

Roie Magen, IT Manager EMEA, TOMIA

Learn how TOMIA protects diverse workloads with Commvault >

"WITH THE **POWER OF COMMVAULT AND METALLIC**, WE ARE CONFIDENT THAT WE ARE PREPARED FOR ANY DISASTER."

Jean Alain Rodriguez, Head of Services Management Office, Evoluti

Learn how Evolutio ensures cyber recovery with Commvault >

eBOOK

TAKE YOUR DATA SECURITY TO

THE NEXT LEVEL

WITH COMMVAULT.

START HERE >

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®