Commvault®

THE HIDDEN COST OF SEVEN TOOLS

A field guide for data center teams who built something worth protecting.

You didn't build your stack overnight. You made smart decisions with the budget and vendors you had. This guide isn't about tearing that down. It's about what it actually costs to keep seven tools running – and what it looks like when one platform does the work instead.

THE STACK YOU BUILT – AND WHY IT MADE SENSE

Nobody sets out to run seven backup tools. You ran one, and it worked. Then the workloads changed. A new cloud provider came in, two more followed. The business acquired something running a different hypervisor. You needed coverage for Kubernetes. Each tool entered the stack because it solved a real problem at a real point in time. You made good calls.

Here's the tension:
The stack that made sense to build doesn't always make sense to run. Not because the technology is bad, but because the operational model compounds over time. Every tool you added brought capability – and brought a console, a policy set, a renewal cycle, and at least one person who knows how it really works.

The average data center team managing legacy backup infrastructure now runs seven or more separate systems. That's not a sign of dysfunction, but the natural result of solving real problems with available tools, over years, across an environment that kept growing.

What it costs to keep that running is a different conversation – one most teams don't have until something goes wrong. Here are some questions you should be thinking about:

- How many environments – on-prem virtualization, public cloud virtual machines, Kubernetes, SaaS, file/object, databases, identity – do you protect today?
- How many consoles does that translate into?
- Can you enforce service level agreements and policies consistently across them?
- If you had 10 minutes to brief the CIO and board on protection and recoverability, could you?

THE BILL YOU CAN SEE – AND THE ONE YOU CAN'T

THAT WAS THEN	THIS IS REAL
Every tool has its own bill. Every vendor wants more at renewal. Storage and cloud costs keep climbing. And those are just the costs you can see.	Lower total cost, without throwing out what you've already paid for. Fewer tools to license. Less storage needed. And the hidden costs come back, too.

The visible costs are painful, but at least they're legible. Per-tool licensing across seven vendors. Storage overhead, with large amounts of data duplicated between primary and secondary sites. Support contracts with separate renewal timelines. You can budget for these, even if the number is uncomfortable.

The hidden costs are harder. They don't show up on an invoice, so they rarely make it into a business case. But every data center team running a multi-tool environment knows exactly what they are.

Engineer hours spent maintaining scripts that bridge what the tools don't natively share. The 2 a.m. call when backup fails and only one person knows how to fix it. Recovery drills that require a war room because the process is too specialized for any single engineer to run solo. The audit request that takes three days to answer because the data lives across four systems in four formats. Renewal negotiations running in parallel across multiple vendors, every year, with no natural leverage point.

None of that shows up on the license invoice. All of it is real cost.

WHAT CONSOLIDATION DELIVERS

Fortune Brands **saved $22.7M –** a **73%** reduction in total cost – through consolidation.[1]

NTT-Netmagic reduced costs by **$300K annually** and cut storage overhead by **35%.**[2]

If you can't see the real bill, it's not real resilience.

[1] Fortune Brands Innovation Achieves 73% Cost Savings with Unified Data Protection
[2] NTT-Netmagic Saves $300,000 Annually with Commvault Cloud: A Cyber Resilience Success

WHAT CONSOLIDATION ACTUALLY LOOKS LIKE

THAT WAS THEN	THIS IS REAL
Forced rip-and-replace. New boxes, new vendors, new procurement. Throw out the storage you bought, the scripts you wrote, the contracts you negotiated. Start over to get started.	No starting over. Works with the storage already in your rack. Start small, expand as contracts run out and budget frees up.

The word “consolidation” makes most infrastructure engineers reach for their calendar. They picture a rip-and-replace project – new hardware, new procurement, a migration that surfaces six months of hidden dependencies and lands at the worst possible time.

That’s not what consolidation has to look like.

The right platform works with the storage already in your rack – not just its own hardware. You don’t have to throw out contracts you negotiated or equipment you haven’t depreciated. You can start where it makes sense:

Commvault Grid for measured, scalable growth in your data center.

Commvault Flex for growing petabyte scale datasets.

Commvault Edge for smaller branch sites.

Commvault Cloud for SaaS applications and cloud workloads, or hosted and delivered as-a-service for your cloud-native or SaaS workloads.

Then you can expand as old contracts run out and budget frees up. Your timeline, your racks, your call.

What you get in return: a single control plane across on-premises, cloud, and hybrid workloads. One set of policies. Centralized management and consistent governance. One place to answer the auditor’s question.

The engineers who were holding seven dashboards together start doing something more useful instead. That’s not a modernization story. It’s an operational-relief story.

If it picks the hardware, it’s not real resilience.

WHAT YOU GET WHEN THE PLATFORM GROWS WITH YOU

THAT WAS THEN	THIS IS REAL
A backup tool that does backup. Bolt something on for ransomware. Bolt something on for governance. By the time you've assembled the answer, you're back to tool sprawl.	One platform that does everything you need now – and everything you'll need it to do next. Recovery that is fast, clean, and provable.

You bought this for backup. That still has to be excellent – and it is. But backup is no longer the full requirement.

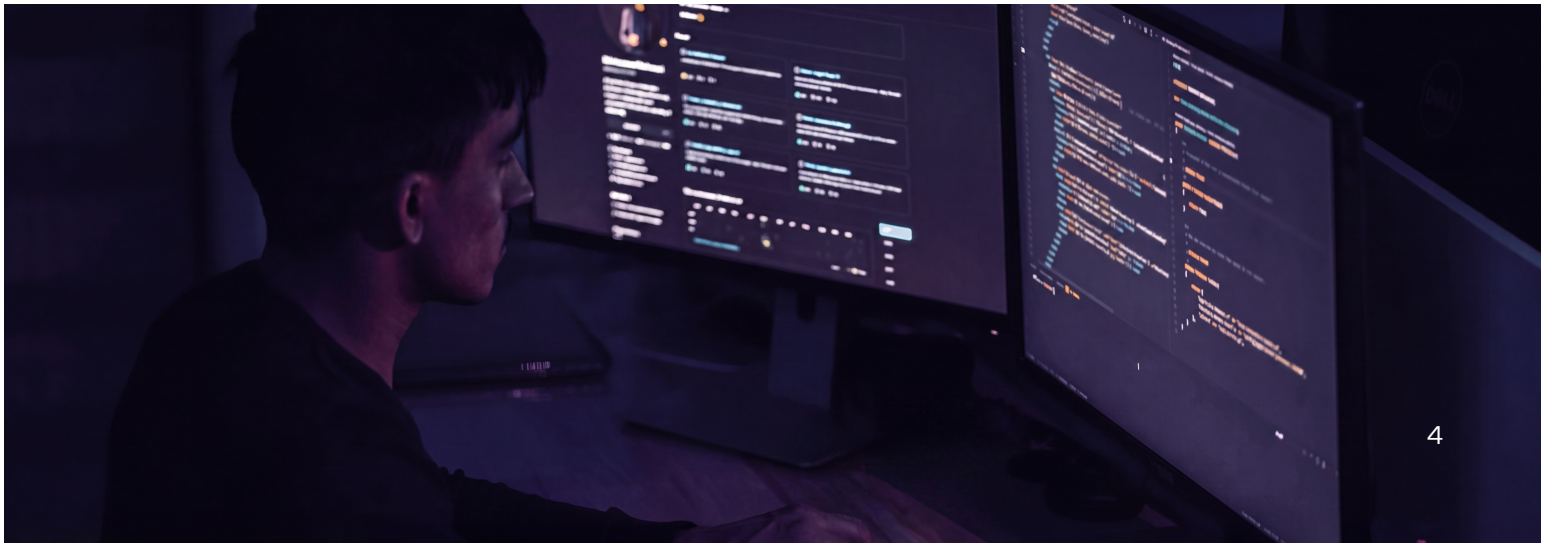
Attackers now target backups specifically. If your backup environment is compromised, your recovery is compromised. Auditors increasingly require proof of recovery capability, not just proof of backup. "We ran a drill last year" doesn't satisfy a regulator who needs documented, tested recovery for a specific workload.

The platform needs to find your data, classify it, protect it, and recover it – cleanly and provably. That's table stakes. What changes with a unified platform is what comes next.

As the threat landscape expands – ransomware, identity threats, AI-era risks your team is only beginning to plan for – Commvault Cloud expands with it. You don't bolt on another tool and restart the consolidation problem. You're already covered.

Cyber readiness isn't the reason to start this conversation. It's the reason you won't have to start over.

If it only protects what you have today, it's not real resilience.



COMMVAULT® CLOUD FOR HYBRID ENVIRONMENTS

Commvault Cloud helps unifies cyber resilience across hybrid environments – on-prem, cloud, and SaaS – through one control plane rather than a patchwork of point tools. It emphasizes policy-driven automation to help scale protection consistently, plus risk assessment, compliance support, and cost visibility/optimization so teams can close coverage gaps and budget with clearer numbers.

Architecturally, it highlights hardened data security (including concepts like immutable/air-gapped protection) and cyber recovery capabilities (such as Threat Scan and Commvault Cleanroom) with deployment flexibility to run the platform in an organization's private cloud or via Commvault's cloud delivery option.

See how Commvault works with the infrastructure you've already built – without the rip and replace.

REQUEST A DEMO →
