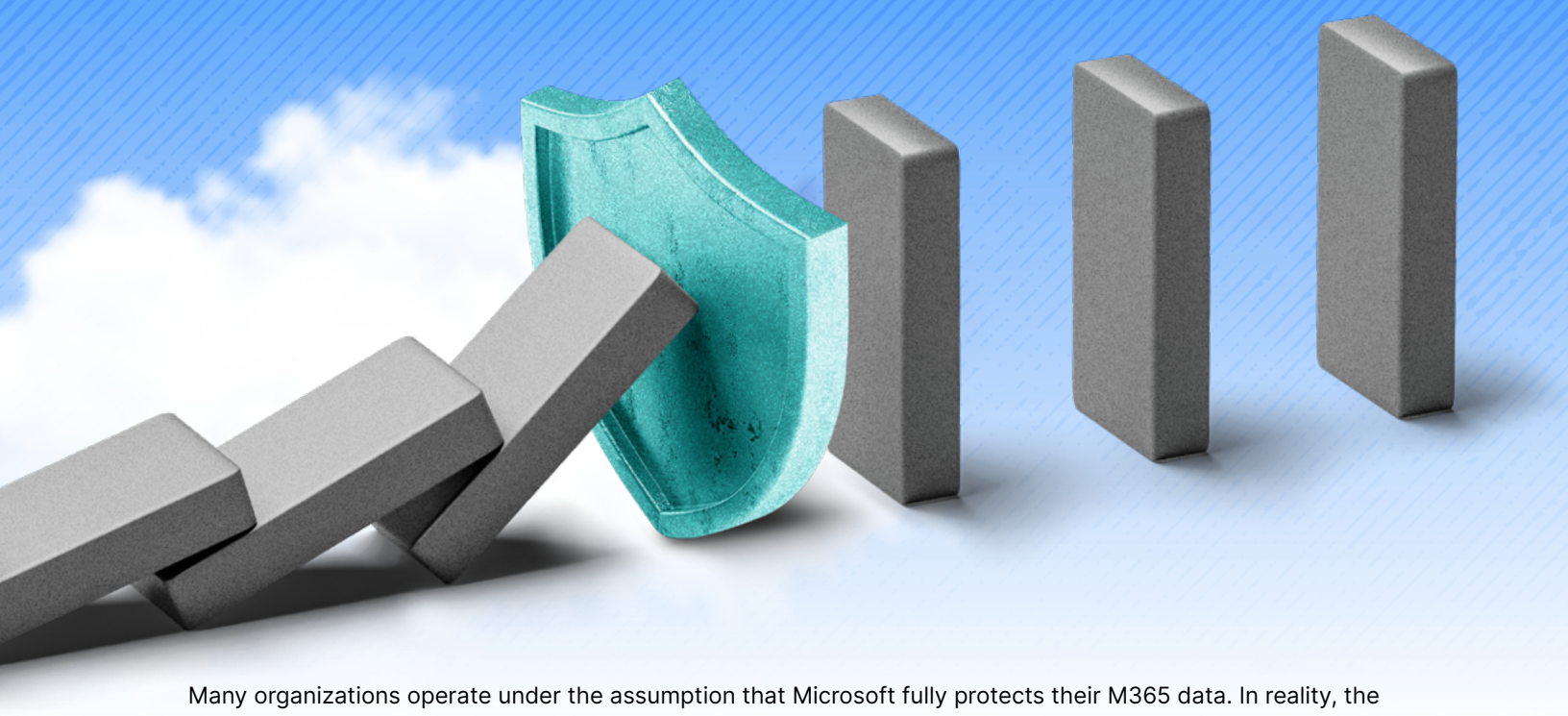
rubrik

THE DAY WITHOUT YOUR M365 DATA

The IT Leader's Playbook for Getting the Business Back Online

When an IT Ticket Becomes a Business Emergency

When Microsoft 365 data is lost, the impact moves faster than most organizations expect. What begins as a routine service disruption — an IT ticket, a service restart — can become a business emergency within hours: revenue stopped, operations stalled, and a recovery clock ticking without a clear answer on where to start.



Many organizations operate under the assumption that Microsoft fully protects their M365 data. In reality, the Microsoft Shared Responsibility Model makes clear that securing and backing up that data is the customer's responsibility. The native tools provided are useful for short-term retention and eDiscovery, but were not built to address the full scope of enterprise data resilience and recovery requirements.

This gap between assumption and reality rarely surfaces until something goes wrong. A service interruption triggers an IT ticket. The apps come back online. And then someone asks for the file — and it isn't there. The SharePoint site twenty people have been building for six months is gone. What began as a routine incident has become a data loss event, with immediate implications for business operations, compliance, and revenue.

According to Rubrik Zero Labs,

94%

of IT and security leaders reported their organization experienced a significant cyberattack last year.

Of that 94%,

64%

were attacked through their SaaS environments — making it the most targeted type of environment.

For organizations that depend on M365, the question is no longer whether data loss can happen. It's whether they're prepared when it does.

Three Ways M365 Data Disappears

M365 data loss is rarely a single, predictable event. It happens in different ways, at different times, and for different reasons — each with its own recovery challenge. For M365 Admins and IT Leaders, understanding the distinct failure modes is the first step toward building a resilience strategy that accounts for all of them.

$4.44M

Average cost of a data breach in U.S.[1]

Cyberattack

Financially motivated cybercriminals increasingly target M365 environments, stealing data and holding it for ransom. Compromised credentials are enough to walk through the front door undetected. No technical vulnerability required.

34%

SaaS data loss caused by accidental deletion[2]

Accidental Deletion

A well-meaning employee cleans up files they didn't realize were critical. A SharePoint site twenty people have been building for six months gets deleted and nobody notices until it's too late.

47%

Increase in AI-enabled cyber attacks in 2025[3]

AI Agent Error

An AI agent executes a task, reorganizing files, bulk-editing data, running an automated workflow, and corrupts data across SharePoint before anyone notices. No alert. No threat signature. By the time it's discovered, the damage has already spread.

Each failure mode lands differently. Each one demands a different recovery. A cyberattack requires identity remediation — removing attacker footprints from Entra ID and AD — before anything comes back online. An accidental deletion requires granular restore capabilities that native tools often can't deliver. An AI agent error requires the ability to pinpoint exactly when the corruption occurred and rewind to a clean state. What they have in common is that none of them announce themselves on your timeline, and none of them wait for you to be ready.

1. (IBM 2025) | 2. 2025 State of SaaS Backup and Recovery Report | 3. DeepStrike: AI Cyber Attack Statistics 2025, Trends, Costs, Defense, October 2025.

Your Backup Wasn't Built for This Moment

Many organizations have M365 backup in place and consider the box checked. The problem is not whether data is being saved. The problem is what happens when you actually need to recover it.

Legacy backup tools were built to answer one question: was the data saved? That is the wrong question. When M365 data is lost, the questions that matter are fundamentally different.

What Legacy Backup Answers

- **Was the data saved?**
- **When was the last backup?**
- **How much data was lost?**
- **Can we restore the files?**

What You Actually Need to Know

- **What do we restore first?**
- **Is the backup clean or compromised?**
- **Which people and workflows need to be back online now?**
- **How do we get the business running again?**

Legacy tools answer the first column. When M365 data is gone, your business is asking the second.

Legacy tools hand you a list of restore points and leave you to figure out the rest. Manual triage under pressure. No guidance on what is actually critical. No safeguard against restoring infected data back into a live environment.

For M365 Admins and IT Leaders, that gap has real consequences. Every hour spent triaging a recovery manually is an hour of operational disruption. Every decision made without clear intelligence about what to restore first is a decision made under pressure, without the full picture.

The native tools Microsoft provides were not built to address this. They were designed for short-term retention and eDiscovery, not for the speed and precision that a business recovery event demands. When the SharePoint site is gone and the business is waiting, a list of restore points is not enough.

MINUTES

IT Impact	Business Impact	Executive Impact
Incident confirmed. Recovery scope unknown.	Workflows stalled. Files inaccessible.	Escalation begins.

HOURS

IT Impact	Business Impact	Executive Impact
Manual triage underway. No clear restore priority.	Revenue stopped. Deadlines missed.	Legal and compliance engaged.

DAYS

IT Impact	Business Impact	Executive Impact
Recovery is still in progress. Backup integrity in question.	Customer commitments at risk. Productivity in freefall.	Board notification. Regulatory exposure.

The longer recovery takes, the further up the organization it travels.

How Rubrik Restores the Business, Not Just the Data

In an era of petabyte-scale SaaS environments, brute force backup is a recipe for weeks of downtime. Rubrik unifies autonomous business recovery, identity resilience, and Copilot resilience into a single platform — so that even if your M365 environment is compromised, your business never stops.

Autonomous Business Recovery

From restoring data to restoring the business

AI-driven identification of your Minimum Viable Business (MVB) for surgical, one-click continuity. Bypasses API bottlenecks that make brute force backup slow at petabyte scale. Critical people and workflows back online first — no manual triage.

Minutes, not weeks

Identity Resilience

Protecting the keys to the kingdom

Automated recovery for Entra ID and AD Forests, including clean-room restoration workflows. Restores users, enterprise apps, groups, and roles as part of the same recovery workflow — so identity and data come back online together, not sequentially.

Identity & data together

Copilot Readiness

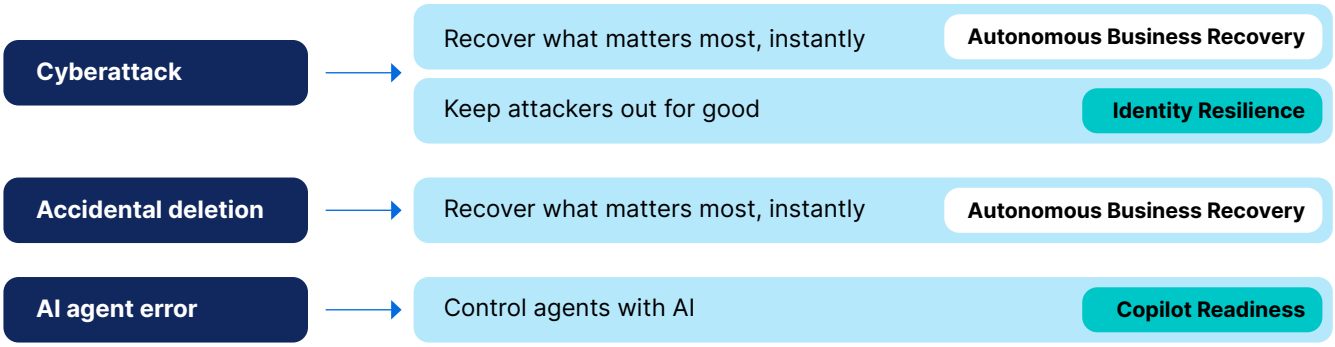
Govern what AI agents see and do

Proactively classifies sensitive data and remediates overexposed links before Copilot starts indexing. Auto-discovers Copilot Studio agents, enforces policies in real time, and provides instant Agent Rewind for destructive AI behaviour — restoring to a clean state before damage compounds.

Proactive, not reactive

Each capability was built for a specific failure mode. Not every incident requires all four — but when the wrong one is missing, recovery stalls.

Which Rubrik capability answers which failure mode



The difference between legacy backup and Rubrik is not just speed. It is the difference between being handed a list of restore points and being guided through a recovery that puts the business first.

Recovery timeline: legacy backup vs. Rubrik

	Legacy Backup	Rubrik
Minutes	Manual triage begins. No restore priority. API bottlenecks slow everything down.	MVB identified automatically. Clean backup confirmed. Identity recovery initiated.
Hours	Still determining scope. Backup integrity unknown. Business impact compounding.	Business back online. Environment clean. Copilot agents discovered and governed. Shadow AI access remediated.
Days	Recovery still underway. Regulatory exposure confirmed. Board notification.	Full recovery complete. Shadow access remediated. Audit trail documented.
Weeks	Up to 2 weeks to full recovery. *$4.44M average cost of a data breach (IBM, 2025)*	Already done.

For M365 Admins and IT Leaders, that timeline is not abstract. Every row in the legacy column is a conversation you do not want to be having — with operations, with legal, with the CEO

What Recovery Looks Like in Practice

The gap between a data loss event and business recovery is where Rubrik's impact is most visible. For M365 Admins and IT Leaders, the measure of a resilience solution is not whether it protects the data. It is whether the business kept running when it mattered most.

City National Bank

Florida's second-largest bank with $22 billion in assets, CNBFL serves 32 branches across the state where 1,000+ employees depend on M365 daily — and where banking clients expect real-time availability 24/7/365.

When ransomware threats against financial services organizations intensified, the stakes were immediate. Client transactions, branch operations, and the bank's ability to serve customers paying bills and managing their livelihoods were all on the line — and downtime was simply not an option.

With Rubrik, CNBFL unified M365 protection for 1,000+ users alongside on-prem and Azure environments in a single platform — giving the CIO full visibility into where data lives at all times and the confidence to keep the bank open no matter what.

"As a bank, we cannot close our doors to our clients. Downtime is not an option. Rubrik allows us to remain agile, staying current with the market demand, and where the bank wants to be from a strategic level."

Ariel Carrión, *CIO, City National Bank of Florida*

1,000+ M365 users protected
24/7/365 availability maintained
$22B in assets secured

VERSPIEREN

France's largest independent insurance broker, Verspieren manages 120TB+ of sensitive customer data and 1,200 M365 users across 25 companies — making continuous data availability essential to serving over 12,000 customers.

When ransomware and cyber threats became a systemic risk to the insurance industry, the stakes were immediate. Millions of sensitive customer files, regulatory compliance obligations, and the continuity of customer-facing services were all on the line.

With Rubrik, Verspieren achieved 24×7×365 protection across both on-prem and SaaS environments, unified under a single platform — fully deployed in under 90 days, with a guaranteed data recovery chain from backup through legal archiving.

"The priority shouldn't be to avoid or prevent a cyber attack. Three key issues need to be addressed: how to guarantee reliable data; how to guarantee continuity of IT resources and services for customers; and how to get back to 100% operations as quickly as possible. Rubrik checked all of those boxes."

Pascal Wronski, *CIO, Verspieren*

<90 days to full deployment
120TB+ of data protected
1,200 M365 users under 24×7×365 coverage

The Only Thing You Can Do Is Save the Day

When M365 data is gone, the clock is already running. For M365 Admins and IT Leaders, that moment is not a technical problem. It is a business problem — revenue stopped, operations stalled, and a conversation with the CEO that nobody wants to have.

The organizations that navigate that moment without lasting damage are not the ones with the most complex backup infrastructure. They are the ones who knew exactly what to restore first, had a clean environment to restore into, and got the business back online before the impact compounded.

That is what Rubrik was built for. Not to check the backup box. Not to hand you a list of restore points and leave you to figure out the rest. To restore the business, not just the data — no matter how the incident started.

With Rubrik, you do not have to figure out which problem you have before you can start solving it. Recovery is guided, not guessed. The environment is clean before data comes back online. And if an AI agent corrupted your data, Rubrik can rewind it — instantly, to the exact moment before it went wrong. And when the business is watching, the only thing you can do is save the day.

Restore your business, not just your data.

See Rubrik for M365 in action → Explore Page

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubriklnc on X (formerly Twitter) and Rubrik on LinkedIn.

A-Day-Without-M365-Data / 20260601