




Protecting the Everywhere Workplace:

Rubrik Brings Zero Trust Data Security to Microsoft 365





Think Your Microsoft 365 Data is Secure? Think Again.

Microsoft 365 is one of the most popular work tools in the world, with more than 258 million monthly active users. As a result, it has become a tempting target for cybercriminals.

Today's hybrid work environments and widespread use of cloud-based technologies have given cybercriminals new attack vectors, and it's difficult for enterprise security teams to keep up. Addressing this challenge requires two shifts in approach. The first shift is accepting that cyberattacks are increasingly a matter of when, not if. The second shift is a move toward a Zero Trust Architecture for Microsoft 365 environments. Companies must have logically air-gapped backups of their Microsoft 365 data, so they never lose their critical workloads, face downtime or have to pay a ransom.

To successfully execute these shifts, they need an effective data protection platform. Rubrik for Microsoft 365 helps organizations become more resilient with an immutable backup that helps them get back to business faster with rapid, reliable recovery.

SECTION ONE

Securing a boundless desk

Traditional perimeter-based approaches to security aren't conducive for hybrid and remote workplaces, leaving the majority of today's work collaboration spaces vulnerable. Seventy-one percent of users have experienced an account takeover, a type of attack where a malicious third-party accesses user account credentials,¹ while 85 percent of users have experienced an email breach.²



Malicious actors can use Microsoft 365 apps as a tunnel into an organization's larger network

Perhaps the riskiest aspect of Microsoft 365 is that it allows malicious actors to bypass authentication barriers with stolen credentials. Once they're authenticated; they're in, and, if they're careful, they can move around the system without triggering any alarms, especially if there are no tools in place to keep an eye on the Microsoft 365 environment.³

Not only is there an overwhelming number of devices to protect, but there's also an overwhelming amount of data. Enterprises are projected to produce 181 zettabytes of data by 2025, up from 5 zettabytes in 2011.⁴



The number of attack vectors and accounts that could be compromised means that protecting vulnerable Microsoft 365 environments requires the right tools and automation.

In order to protect Microsoft 365 environments, organizations need:

1. Verification tools for every network entry point and user
 2. Trusted recovery points with secured primary data sources and viable backups in the face of internal and external threats
-

The complexity of Microsoft 365 environments and the number of integrations they have makes it difficult for enterprise security teams to be on guard for all possible threats—including lateral movements and the suspicious use of tools such as Power Automate or eDiscovery.⁵

How can organizations effectively protect their growing Microsoft 365 environments? Rubrik for Microsoft 365 implements a Zero Trust Architecture that secures your current workloads and shields your backups from reinfection.





Rubrik for Microsoft 365: Zero Trust Data Security

Adopting Zero Trust is what allows organizations to manage numerous devices and users all at the same time.

Zero Trust Architecture takes a “trust nothing, verify everything” attitude to security. This framework makes sense when you consider that users are increasingly logging on from personal computers, home networks, and coffee shops. Even if a user is innocent, the device they use to access the organization’s network may have already been compromised by a malicious actor.

Throw in the number of people who use Microsoft 365—over 1 billion people currently use a Microsoft Office product or service⁶—and it’s easy to see why managing this sprawling environment of users and devices has become so complicated.

Rubrik’s Zero Trust Data Security rests on three principles:⁷

1. **Verify explicitly:** Security decisions are made based on all available data points, including identity, location, device health, data classification, and anomalies.
2. **Use least-privileged access:** Just-in-time and just-enough access are given, so people have the access they need to do their jobs and nothing more.
3. **Assume a breach:** All access is treated as if it’s a potential breach, meaning the potential exposure is minimized using micro-segmentation, continuous monitoring, end-to-end encryption, and automated threat detection.

Building a cybersecurity policy on the pillars of Rubrik's Zero Trust Data Security enables organizations to:

Develop a single, user-friendly view of the Microsoft 365 environment

Security teams can't oversee a thousand things at once. It helps to have a centralized view of privileged Microsoft 365 accounts, especially those with access to sensitive data or specialized Microsoft 365 tools like eDiscovery.

Backup in the cloud for business continuity

On-premises storage methods put business continuity at risk, with no option for restoring Microsoft 365 data on-premises. Managing and maintaining additional infrastructure and backups and the potential exposure of SaaS backups to threat actors introduce further complexity and cause for concern. Organizations need a data backup and protection platform that can automatically protect new users and teams.

Create actionable metrics

Simply gathering data and tracking certain security metrics is not enough. Instead, organizations need actionable metrics where the information gathered is used to trigger specific actions.

Introduce multi-factor authentication

Require users to use both a password and a separate device or item, such as their phone or their fingerprint, to authenticate themselves.





Obtain a unified, user-friendly view of all environments

A single pane-of-glass environment with a user-friendly interface makes it simple for security teams to identify, archive, and replicate data from Microsoft 365 environments as well as assign RPOs and retention periods based on business needs.

Use an intuitive data protection platform

One of the most challenging things about the Zero Trust security framework is managing different environments and devices with all the steps required to verify permissions and grant access. With an intuitive platform, cybersecurity professionals have access to greater levels of abstraction and can easily create backups of all necessary systems.

Create immutable data backups

Once data backups are created, they must not be compromised. Keeping backups secure requires a platform that creates immutable data backups which cannot be altered once stored. If, for any reason, compromised data is ingested into the backups, no previous backups are affected.

Provide one data protection platform for seamless work-from-anywhere environments

With one data protection platform for any working operation (e.g., in-office, hybrid, or remote), employees can work from anywhere in the world, even in the event of a business interruption, while using the same tools and enjoying the same level of protection and access.

SECTION TWO

Here's how Rubrik for Microsoft 365 fills in the gaps for your shared data responsibility model:

While Microsoft's native protections are useful for data governance and retention, they are not designed to help with threats such as accidental deletions or attacks from malicious actors. Organizations using Microsoft 365 need a third-party solution to supplement the data governance and management tools they already enjoy from Microsoft.

Rubrik Zero Trust Data Security, a data management and cyber resilience platform, offers this additional layer of protection to Azure environments.





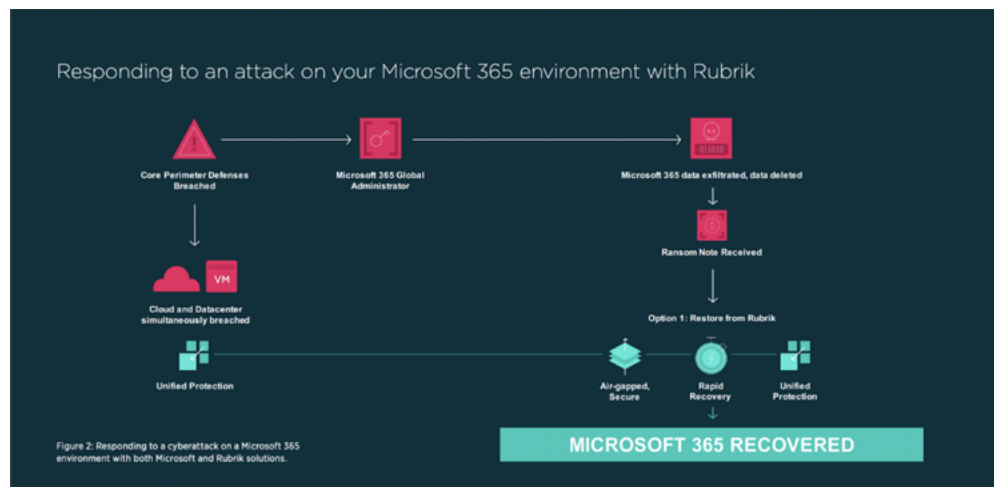
Help ensure complete data protection across your Microsoft 365 ecosystem.

Choosing a third-party data security platform for Microsoft 365 is not only a best practice but one recommended by Microsoft; it's even mentioned in the service agreement.⁸ If you've got measures in place to recover on-premises data from ransomware, malicious internal actors, or even accidental deletions of critical files, it's important to check whether you've got the same level of protection for your Microsoft 365 data. Are you prepared to recover that?

You can be with Rubrik for Microsoft 365.

Rubrik is supported by a core set of technologies that sets it apart from legacy backup solutions:

- **Immutable data platform:** No external or internal operation can modify data once it's been ingested. Data managed by Rubrik is never available in a writable state to the client. Backups can't be overwritten, so even if infected data is ingested by Rubrik, it can't infect clean files and folders.
- **Declarative policy engine:** Rubrik makes it simple for organizations to carry out their data protection activities. With the declarative policy engine, they can work with simple input fields to set RPO, retention period, archive target, and replication target.
- **Threat engine:** Organizations get a full perspective of what's going on in each workload thanks to machine learning that analyzes each backup snapshot's metadata. Rubrik detects anomalies, analyzes threats, and accelerates recovery from adverse events.
- **Secure API-first architecture:** Rubrik has an API-driven architecture. The Rubrik platform is built on top of a rich suite of RESTful APIs, allowing easy integration with third-party services. All user activity in the Rubrik platform is logged and made available to administrators through both the Rubrik UI and APIs.



Rubrik for Microsoft 365 provides a more comprehensive solution—the convenience of Microsoft tools with the ironclad protection of Rubrik’s Zero Trust Data Security platform.

When the cloud and data center are breached, the system administrator can log into their Rubrik account for an air-gapped, secure backup of their data. So, while Rubrik automatically ingests data from the Microsoft 365 environment, that backup can only be accessed through Rubrik using two-factor authentication and role-based access control. Attackers have no way to modify the backups and organizations can rapidly recover their data without paying the ransom.





Top building contractor reduces Microsoft 365 data recovery time from hours to minutes

When JE Dunn, one of the top building contractors in the U.S., decided to upgrade its backup systems, it turned to Rubrik. JE Dunn's information technology systems were critical to delivering customer projects, but its aging tape backup software was struggling to keep up with its 99% virtualized environment. The company chose Rubrik, not just for its innovative backup and recovery solutions, but for its API-first architecture, automation, and orchestration.

Its APIs made it easier for less technical engineers to work with Rubrik and deliver business value. JE Dunn was able to protect Microsoft 365 while keeping its data in Azure, so it had complete control over where the data was stored. The company enjoyed 62% TCO savings, 90% management time savings, a 75% reduction in data center footprint, and reduced recovery time from hours to minutes.

“With our previous solution, it could take hours to recover. With Rubrik, we’re able to satisfy most requests in less than 10 minutes. Outside departments are recognizing the solution as an important tool for recovering lost work.”

-Jason Hull Senior Systems Manager

San Joaquin County replaces several backup solutions with Rubrik's standard platform

San Joaquin County (SJC) can't afford any downtime. With public services from law enforcement to public assistance relying on its IT systems, it needs to ensure it can get back up and running immediately in the event of a disruption. In the past, SJC relied on time-consuming and costly tape backups, and the Assistant CIO wasn't convinced this approach was secure or accessible enough. SJC originally used Cohesity to manage tape backups of its Office 365 mailboxes but were unable to back up 40% of the targeted data.

When the Assistant CIO started looking at Rubrik, he was impressed by the fact that it offered everything he was currently getting with Cohesity plus immutability—which provided peace of mind should the county ever fall victim to a ransomware attack. The result was 40% TCO savings, a full-time IT employee who could be reallocated to strategic initiatives, and a reduction in restore time from 12 hours to minutes.

“We were able to replace multiple backup solutions with a standardized data management platform across all departments.”

-David Newaj Assistant CIO for SJC





Adopting Rubrik for Microsoft 365 gives you the perfect pair for a wraparound Zero Trust solution. Your organization can enjoy the multi-faceted work environment of Microsoft 365 and the user-friendly experience of the Rubrik Zero Trust Data Security platform.

Want to learn more about how to protect your Microsoft 365 environment with truly reliable backups? Get in touch with a member of the Rubrik team.

Start your free trial today

References

1. Office 365 Security Takeaways E-Book: Security Microsoft Office 365 in the New Normal:
<https://www.vectra.ai/forms/office365-survey-ebook>
2. Preventing email data loss in Microsoft 365:
https://www.egress.com/media/2k4ffksv/egress-report_preventing-email-data-loss-in-microsoft-365_1221.pdf
3. Cyberattacks Use Office 365 to Target Supply Chain:
<https://securityintelligence.com/articles/cyberattacks-office-365-supply-chain/>
4. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025:
<https://www.statista.com/statistics/871513/worldwide-data-created/>
5. Microsoft Office 365 Accounts a Big Target for Attackers:
<https://www.darkreading.com/vulnerabilities-threats/microsoft-office-365-accounts-a-big-target-for-attackers>
6. Over 1 billion people worldwide use a MS Office product or service:
<https://financialpost.com/personal-finance/business-essentials/over-1-billion-people-worldwide-use-a-ms-office-product-or-service>
7. Evolving Zero Trust: How real-world deployments and attacks are shaping the future of Zero Trust strategies:
<https://www.microsoft.com/en-us/security/business/zero-trust>
8. Microsoft Services Agreement:
<https://www.microsoft.com/en-us/servicesagreement>