rubrik | Microsoft

Is Your Desk Safe? How Zero Trust Data Security Protects Your Microsoft 365 Environment

Introduction

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. Organizations are only now realizing how vulnerable their workplace collaboration spaces are. 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 81 percent of users have experienced an email breach.[2]

Today's hybrid work environments and widespread use of cloud-based technologies have given cybercriminals new attack vectors, and it's challenging 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 towards a Zero Trust framework for Microsoft 365 environments. Companies must have logically air-gapped backups of their Microsoft 365 data, so they can regain operations and never pay a ransom. To successfully execute these shifts, they need an effective data protection platform. Together, Rubrik and Microsoft help prepare organizations to not only meet compliance goals, but also respond to attacks with rapid, trusted recovery.

Chapter One

As far as popularity contests go, Microsoft 365 is a clear winner when it comes to workplace collaboration tools. The cloud service combines many of the word processing and email tools modern workers are most familiar with while providing additional productivity applications and AI-powered features.

Despite this transition into digital workplaces, old-fashioned thinking around these tools remains. It's only recently that organizations have caught on to the fact that their Microsoft 365 environments are high-value targets for cybercriminals.

"Microsoft 365 is a gold mine," said Doug Bienstock, an incident response manager and speaker at Black Hat USA 2021. "The vast majority of [an organization's] data is probably going to be in Microsoft 365, whether it's in the contents of individual emails, files shared on SharePoint or OneDrive, or even Teams messages."[3]

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

In 2019, hackers targeted Microsoft 365 administrators with fake alerts that said their licenses had expired. The administrators clicked on a link leading them to what they thought was a login page where they could update their payment information. Instead, their user credentials were stolen.[4]

In 2020, attackers sent emails that looked like they came from the U.S. Supreme Court. These emails intimidated recipients into clicking a "View Subpoena" button that led to a page asking for user credentials.[5]

With these credentials in hand, malicious actors find a way to leverage that initial win into an even larger win. At first, access to an employee's email or documents may not seem devastating, but that information gives hackers the power to pass themselves off as legitimate employees and gain further access into not just the initial organization, but affiliated organizations as well. For instance, an attacker might use their access to an employee's email to send outgoing messages with the intent of compromising external vendors or customers.[6]

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.[7] And these kinds of threats can only be managed with precisely designed tools. 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 the past, companies protected their Microsoft 365 environments using a castle-and-moat approach. This approach assumes that anyone within the network perimeter is safe, so all resources go towards monitoring and re-enforcing entry points to the network. The problem is that companies are increasingly working in hybrid or remote environments where users and devices are widely distributed, and therefore aren't entirely compatible with the perimeter-based approach. Moreover, common workarounds such as VPNs were designed for remote work in a pre-cloud computing era; SaaS services without a physically controlled data center require a new paradigm of protection.

Then there's a common, but often overlooked, source of data loss: accidental deletions. Accidental deletions take many forms. An employee may have meant to perform one function only to erase a file altogether. Sometimes, they intentionally delete an email or file in an effort to save space or clean up their folders, because they mistakenly assume it's no longer needed. Accidental deletions differ from malicious intent because the individual doesn't have any nefarious intentions. In other words, they're not trying to hide information, cause the organization harm, or collect a ransom. That said, an accidental deletion can be just as detrimental as an intentional deletion if the lost data can't be recovered.

These are new needs, requiring a new paradigm of Microsoft 365 protection that rests on two pillars:

1. Implementing protection and detection tools for every network entry point and user
2. Protecting not just primary data sources, but their backups as well, in the face of internal and external threats

Of course, this is easier said than done. Not only is there an overwhelming number of devices to protect, 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.[8] Moreover, 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.[9]

How can organizations effectively protect and oversee their Microsoft 365 environments? The key is embracing a new security framework that's progressively replacing the perimeter-based approach: the Zero Trust security framework.

Chapter Two

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

The Zero Trust security framework takes a "trust nothing, verify everything" attitude to security. It doesn't matter if you're inside or outside of the perimeter. 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 service[10]—and it's easy to see why managing this sprawling environment of users and devices has become so complicated.

The Zero Trust security framework rests on three principles:[11]

- **Verify explicitly:** Security decisions are made based on all available data points, including identity, location, device health, data classification, and anomalies.
- **Use least-privileged access:** Just-in-time and just-enough access is given, so people have the access they need to do their jobs and nothing more.
- **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 and response.

Building a cybersecurity policy on this framework has enormous benefits for protecting every entry point in a Microsoft 365 ecosystem, empowering 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.

Chapter Three

Keeping your finger on the pulse of every user and device in your Microsoft 365 environment is possible—with the right platform.

Microsoft's native protection applies to data governance and retention. For instance, if your organization needs to keep its Microsoft 365 data for a certain length of time, Microsoft provides tools to help you automate this process and delete data when it is no longer needed. While these tools are useful for an audit, 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. The best way to understand the power of this protection is to consider the options available to an organization in the event of an attack with and without Rubrik.

Responding to an attack on your Microsoft 365 environment without Rubrik

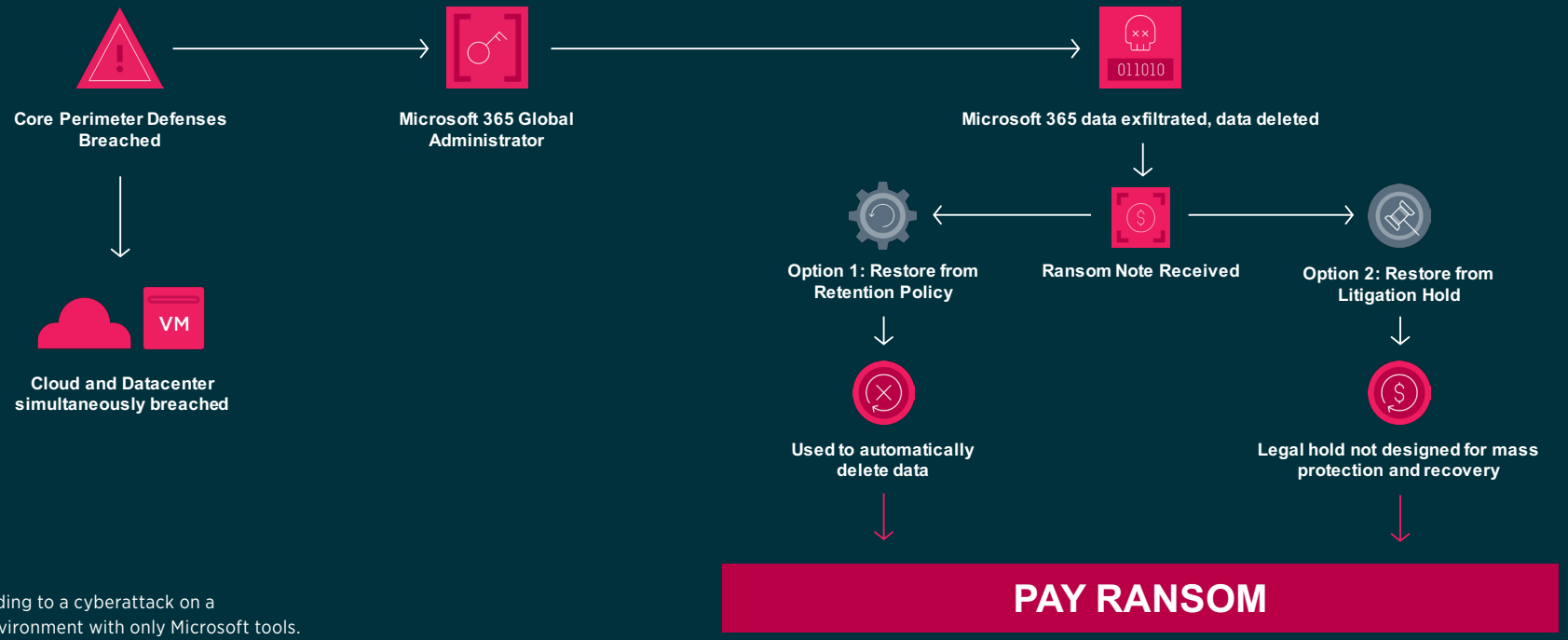

Figure 1: Responding to a cyberattack on a Microsoft 365 environment with only Microsoft tools.

Suppose your cloud and data center are simultaneously breached, leading to the deletion or exfiltration of Microsoft 365 data. **With only the data management and governance tools available in Microsoft 365, you have two potential options:**

1. Restore from your Retention Policy
2. Restore from Litigation Hold

The problem is that the Retention Policy is only designed to hold data for a predetermined amount of time and is used to automatically delete data. Also, your attackers may have compromised this functionality, using it to delete ransomed files.

Complicating matters is the fact that Litigation Hold is not designed for mass protection and recovery. It's targeted to a specific amount and type of data (usually emails and files) that don't need to be rapidly restored.

The only option available to the organization in this case is to pay the ransom.

Responding to an attack on your Microsoft 365 environment with Rubrik

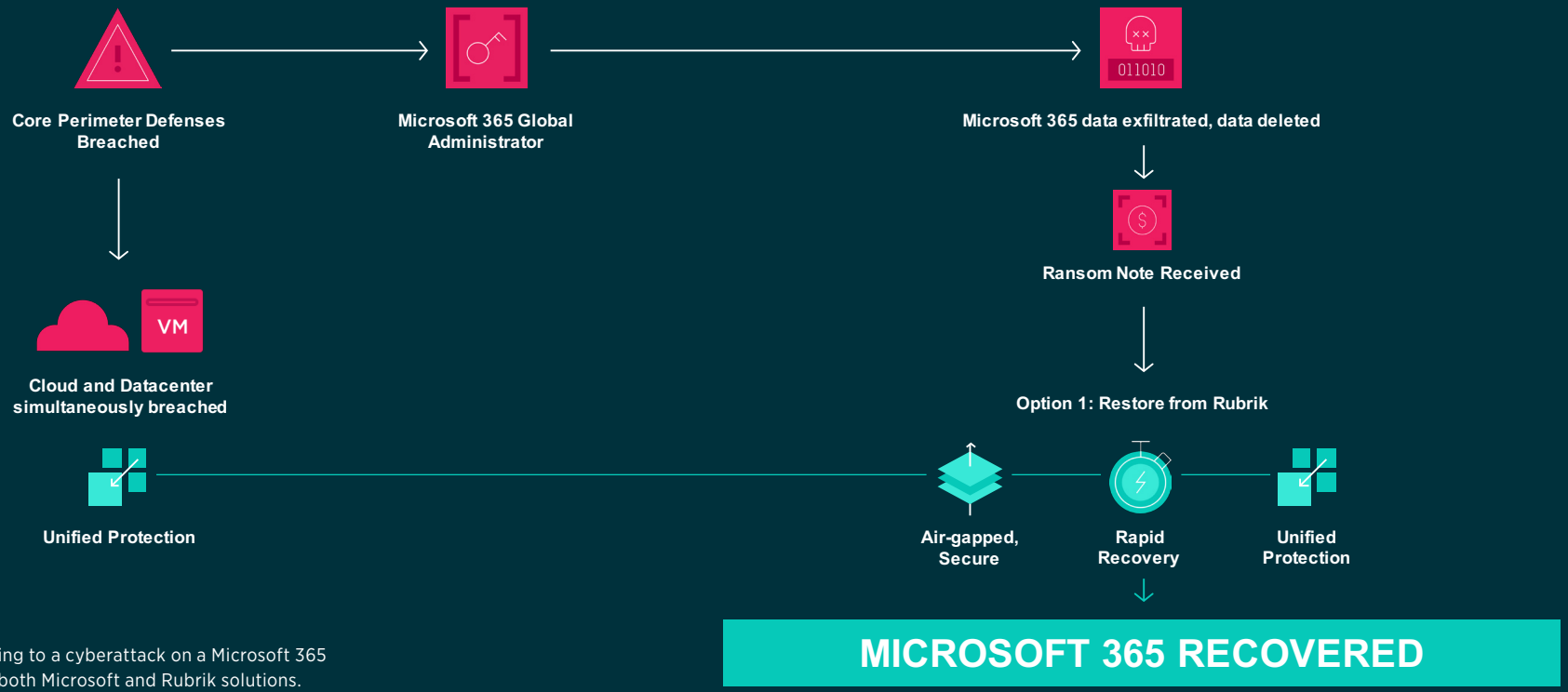

Figure 2: Responding to a cyberattack on a Microsoft 365 environment with both Microsoft and Rubrik solutions.

Microsoft paired with Rubrik 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 where they enjoy unified protection and 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.

> 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

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.

Microsoft recommends regular backups using third-party apps and services

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.[12] 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. 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.

> We were able to replace multiple backup solutions with a standardized data management platform across all departments."
>
> **David Newaj**
> Assistant CIO for SJC

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 re-allocated to strategic initiatives, and a reduction in restore time from 12 hours to minutes.

Adopting Rubrik with 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.

Interested in giving Rubrik a spin?
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 Office 365 Security Takeaways E-Book: Security Microsoft Office 365 in the New Normal:
https://www.vectra.ai/forms/office365-survey-ebook

3 The most dangerous (and interesting) Microsoft 365 attacks:
https://www.csoonline.com/article/3628330/the-most-dangerous-and-interesting-microsoft-365-attacks.html

4 Cyberattacks Use Office 365 to Target Supply Chain:
https://securityintelligence.com/articles/cyberattacks-office-365-supply-chain/

5 Cyberattacks Use Office 365 to Target Supply Chain:
https://securityintelligence.com/articles/cyberattacks-office-365-supply-chain/

6 Cyberattacks Use Office 365 to Target Supply Chain:
https://securityintelligence.com/articles/cyberattacks-office-365-supply-chain/

7 Cyberattacks Use Office 365 to Target Supply Chain:
https://securityintelligence.com/articles/cyberattacks-office-365-supply-chain/

8 Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025:
https://www.statista.com/statistics/871513/worldwide-data-created/

9 Microsoft Office 365 Accounts a Big Target for Attackers:
https://www.darkreading.com/vulnerabilities-threats/microsoft-office-365-accounts-a-big-target-for-attackers

10 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

11 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

12 Microsoft Services Agreement:
https://www.microsoft.com/en-us/servicesagreement