WHITE PAPER

Protect Microsoft 365 With a Zero Trust Approach to Security and Recovery

Hackers are increasingly targeting the popular suite, requiring that enterprises take a more robust approach to securing users and data.





Microsoft 365—one of the most popular work suites in the business world—is also an attractive target for criminals because it contains so much valuable, sensitive information. Hackers can commit many different types of damaging acts on the suite, including locking up the access to the system in a ransomware attack or breaching it and deleting important files.

Many organizations are not prepared for the loss of access to critical files and data that can result from a ransomware attack. That's where a modern security strategy that incorporates Zero Trust (ZT) architecture can help.

By incorporating ZT principles, data is logically air-gapped, and safeguarded from unauthorized access so it cannot be modified, encrypted, or deleted. Simply put: Zero Trust gets in front of hackers with a "never trust, always verify" philosophy when it comes to access control. In order to gain this ZT approach, third-party data protection is essential.

The Attack Landscape Facing M365

When most people were forced to work remotely, Microsoft 365 became part of the toolbox and support strategy to help employees remain productive. Research from Vectra found 97% of organizations extended their Microsoft suite utilization as a result of the pandemic.

This massive growth has also translated into a massive attack surface. Hackers recognize Microsoft 365 as a wealth of opportunity. In fact, in a recent presentation by Mandiant, researchers noted that targeted threat actors are investing a lot of time and money into understanding the application suite and its weaknesses.

Hackers can exploit Microsoft 365 in multiple ways:

1. Email abuse and exploitation of app registration

Data from <u>Egress</u> reveals 85% of organizations using Microsoft 365 have suffered email data breaches. Once inside, criminals can disable mailbox audit logs by abusing mailbox folder permissions, utilizing the proper access level of one user to grant mailbox folder privileges to others.

Bad actors can also compromise Microsoft 365 app registration linked to tenants in order to conduct mass data exportation. They can identify an existing service principal inside of a tenant to hijack access, adding MS Graph application permissions that allow them to read mail and files within the tenants.

To authenticate, attackers then add secrets or certificates as their new credentials. Those credentials act as their API (application programming interface) keys for remote access to make API calls to MS Graph. From there, they can access the last 24 hours of emails from a set group of mailboxes.

85%

of organizations using Microsoft 365 have experienced email breaches.

2. Golden SAML Techniques

Attackers also use Active Directory Federation Services (AD FS) token sign-in keys to gain access to SAML (Security Assertion Markup Language) tokens. For example, hackers responsible for the SolarWinds breach were able to gain access to Microsoft 365 by modifying permissions using the Golden <u>SAML technique</u>, swiping the AD FS sign-in certificate to create tokens for unauthorized users, bypassing two-factor authentication and conditional access policies to access the Microsoft 365 environment. Researchers observed this method still in practice more than a year later.

3. Account takeover

Vectra research found that 71% of organizations have experienced a Microsoft 365 account takeover. Attackers can gain permissions, such as administrator access, by performing an account takeover attack and then compromising administrator credentials. From there, access is boundless, and damage can be deep.

4. Ransomware attacks

Microsoft 365 systems are lucrative targets for the criminals that gain access to multiple corporate systems through ransomware attacks. Once in, hackers often look for backups because they know how crucial that data is to the health of the company. Microsoft itself <u>advises 365 users</u> to invest in third-party backup in order to be prepared for full ransomware recovery.

of organizations using Microsoft 365 have experienced account takeover

Obstacles to Recovery When Microsoft 365 is Compromised

It's a scenario no security leader wants to face: Hackers have breached systems and compromised Microsoft 365 and, with it, a gold mine of sensitive and private data.

Unfortunately, file recovery is often difficult when this happens. In an account takeover, Microsoft 365 retention policies can actually be used against you by an attacker to manipulate and delete policies and data.

If files are corrupted or lost, certain data may not be recoverable without thirdparty backup. For example, Exchange Online files can be permanently deleted after 30 days. Files may be deleted from the Recycle Bin in SharePoint after three months. Often when users attempt to recover files without third-party backup, they lack a separate copy of data stored outside the account, leaving them without recourse if files are destroyed.

While there are some features for safely storing backup, they are not equipped for recovery. The Litigation Hold feature in Microsoft 365 is designed to preserve user data for eDiscovery, not as a means to backup or restore lost data. It cannot be used as a substitute.

4

Additionally, placing all 365 data in litigation hold can create a significant problem when the business is actually subject to an eDiscovery request. All of the data would be deemed discoverable—not just data related to the legal action. This could introduce potential liability that the business' legal team did not anticipate.

These scenarios showcase why it is imperative to have a reliable, third-party backup to restore critical data and ensure business continuity. It is also essential to have a full view of cloud security posture—not only of primary data sources, but also of backups to ensure they are safe and can be restored quickly.

Preventing Damaging Microsoft 365 Attacks

Today's attack landscape requires a Zero Trust approach, which moves beyond simply blocking off networks and systems behind a secure perimeter. ZT assumes systems have already been penetrated; it seeks to lessen potential damage.

Microsoft says the tools used to drive Zero Trust implementations include:

- Strong authentication
- Policy-based adaptive access
- Micro-segmentation
- Automation
- Intelligence
- Data classification and protection

Rubrik Protection for Microsoft 365 offers organizations the ability to securely protect, recover, and archive their Microsoft 365 suite with Rubrik Zero Trust Data Security.



At its core, Rubrik technology comprises policy definition and enforcement points that never expose backup data via open protocols. It supports a purpose-built file system that creates a logical air gap that blocks data from being discoverable or accessible over the network. The solution first identifies authorized users via multifactor authentication (MFA). The policy engine then grants least-privilege access based on the user's specific role with robust rolebased access controls (RBACs). In this way, Rubrik's Zero Trust Data Security combines user verification with policy-based data protection.

A logical air gap enforces multiple data protection functionalities, including a core tenet of the Zero Trust framework: user and employee risk management. This is possible through authentication. MFA safeguards the system from attackers, even when credentials are compromised. Rubrik features builtin MFA. This control enables the careful user verification that is required for success with the Zero Trust model.

Attackers cannot gain access to Rubrik-managed data even if they have stolen credentials to the domain. For legitimate users, RBAC governs access to data, enforcing least-privilege access. The solution only grants access for whatever specific actions that the user needs to perform, as defined by policy. Rubrik secures communications to all system interfaces, including command-line interface and API access.

Additionally, the logical air gap enforces:

- **Authorization.** Fine-grained RBAC enables the principle of least privilege to prevent users from moving laterally within the system to gain unauthorized access to resources.
- Audit logging. Operations are logged and can be monitored locally or shipped to a log analysis tool so there is an audit trail when changes are made within the system.

In addition, Rubrik's solution is delivered as a software-as-a-service (SaaS) application to automatically scale to meet the needs of the modern enterprise and eliminate manual job scheduling. It's simple to scale policy management across tens of thousands of users and add new users with automatic protection. Organizations can also easily locate data with real-time global search, and even recover in bulk or use a granular, three-step recovery to any destination.

Best of all, they can manage everything through one platform, for on-premises and cloud environments.

As attackers increasingly target Microsoft 365 environments, organizations require a robust strategy to counter criminals' efforts. A Zero Trust approach that incorporates data protection and security with robust backup ensures that enterprises protect not only their users, but also their most sensitive data.

Learn more

5

Rubrik builds on Microsoft's native tooling with comprehensive backups and recovery automation to safeguard from data loss and facilitate streamlined management of Microsoft 365 applications.

Learn how Rubrik keeps data secure across the suite of Microsoft 365 applications by visiting Rubrik.com.



