Surviving Common Office 365 Security Pitfalls

IS YOUR ON-PREMISE AD THE WEAKEST LINK?

An IT Pro's Guide

TO SECURING YOUR ON-PREMISE ACTIVE DIRECTORY IN A HYBRID ENVIRONMENT.

Quest

INTRODUCTION

Office 365 has more than **60 MILLION ACTIVE MONTHLY USERS**, and adoption of the platform is increasing—for good reason. It allows organizations to reduce infrastructure and costs related to licensing and maintenance, while expanding storage efficiencies. Additionally, Office 365 empowers workforces to operate from anywhere and from any device, while increasing scalability and business continuity.

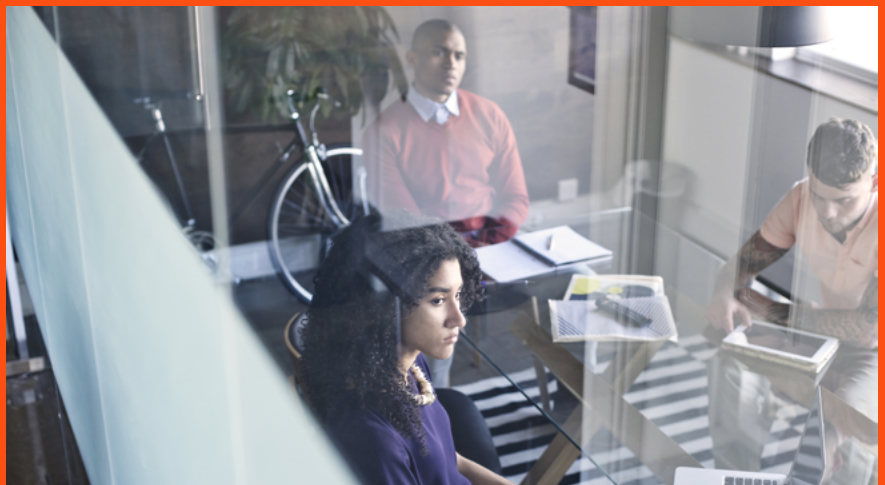
However, moving from an on-premise Active Directory (AD) to a cloud-based directory, like Office 365's Azure AD, still gives some decision makers pause for a common reason—security. As we know, security breaches can negatively impact a company's bottom line (and damage a company's reputation).

In 2016, research by the Ponemon Institute, found that the average cost of a data breach was $4 million per incident.

INTRODUCTION (cont.)

Where should your security concerns be directed? Microsoft promises a financially-backed, 99.9% service-level agreement for Office 365—however, change control, access governance and overall data security is still the responsibility of customers. And the rise of hybrid AD compounds this concern. Think about this: 75% of Office 365 customers with more than 500 users will sync their on-premise AD with Azure AD, creating a hybrid AD environment.

This scenario can lead to dangerous gaps and crippling inefficiencies. Any weaknesses in how the on-premise AD is configured will carry over to Azure AD. Organizations face all the security limitations of native AD and Azure AD, doubling the surface area they need to manage to prevent potential data breaches and insider threats.



INTRODUCTION (cont.)

Securing the data

Securing the data you store in a hybrid environment means taking the necessary steps to secure your on-premise AD—from pre-migration to post-migration. This eBook will identify steps for prepping the on-premise AD for synchronization with Azure AD, protecting data during migration and offer best practices for maintaining a more secure hybrid environment.

PRE-MIGRATION: GETTING YOUR HOUSE IN ORDER

Many organizations work under the assumption that breaches and other forms of data loss are assumed costs of doing business and employ strategies to minimize risk. Prior to migration, data stored in the on-premise AD should be thoroughly assessed and consolidated to eliminate outdated or non-essential items. Your three goals during this process should be:

- **Shrinking your target**—Keep only what users need and eliminate data no longer required for business or compliance reasons; outdated data serves no purpose other than increasing your risk of exposure and non-compliance.
- **Scrutinizing user accounts**—Eliminate duplicate IDs and inactive accounts, match user principle names to domain names planned for use in Office 365 and remediate temporary access that may have been granted to users to test Office 365 capabilities.
- **Tightening access protocols**—Identify weak passwords and require end-users to strengthen them, update admin rights to reflect current staff and bring user data access up to date.

IT Pro Tip

Microsoft's IDFix will help eliminate account duplicity by identifying and remediating object errors in the on-premise Active Directory prior to synchronizing users, contacts and groups into the Microsoft Office 365 environment.

MIGRATION: KEEPING AN EYE ON THE DATA

Once excess data and duplicative accounts have been addressed, access issues have been resolved and security protocols have been met, you're ready to migrate to Office 365. While most of the heavy lifting has already been done, keen attention throughout the migration process will ensure data remains uncompromised. IT admins should have real-time auditing, reporting and alerting to changes during migration to ensure data security. Here are three things to watch:

- **Access**—Companies often use third-party consultants to assist with migration, which could mean temporary access granted to those outside of the organization.
- **Legal holds**—There will likely be data in transit retained for legal purposes, such as archived email or Outlook PSTs; it's critical that a clear chain of custody is recorded to minimize any legal or compliance risk.
- **Issues**—If any abnormalities related to the data in transfer arise—such as data accessed by non-approved users—respond immediately to fix the issue. When it comes to critical data, "better safe than sorry" is always the rule.

IT Pro Tip

Migration to Office 365 offers the opportunity to review your current solution providers. Each vendor should provide options for handling sensitive data throughout the migration to ensure the integrity of your data throughout its lifecycle. If that's not the case, they may not have your best interests in mind.

Post-migration: Maintaining security moving forward

Migration to a hybrid AD environment offers a unique—yet arduous—opportunity to reduce risk associated with excess data, out-of-date permissions/access and duplicative user accounts in your on-premise AD. Now that the "house is in order," here are four post-migration best practices that create a lifecycle methodology for maintaining the organized environment you've created:

1. Continually assess
2. Detect and alert
3. Remediate and mitigate
4. Investigate and recover

POST-MIGRATION: CONTINUALLY ASSESS

1 Continually Assess

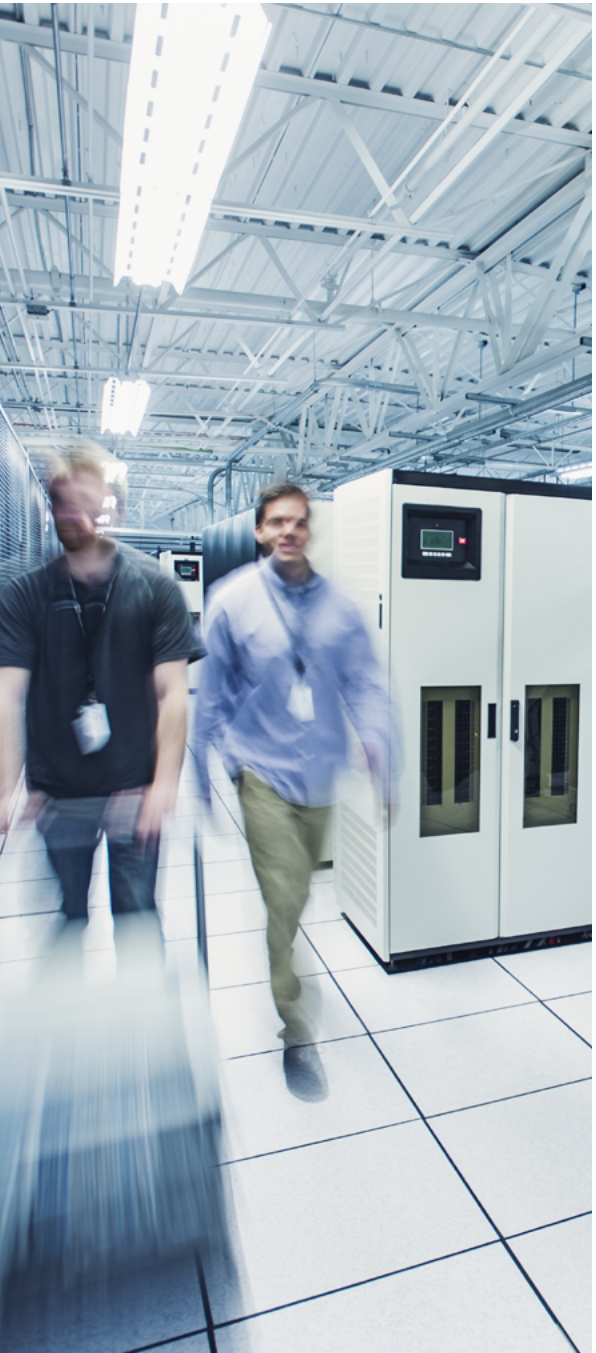
Auditing your hybrid environment is critical to understanding who has access to permissions, privileged groups, sensitive business groups, group policy objects (GPO) and data at all times. A thorough assessment of your on-premise AD and Azure AD should allow you to easily identify:

- Your surface attack area, vulnerabilities and risk profile
- Who has access to what sensitive data
- How they got access
- Who has elevated privileged permissions in AD, servers and SQL DBs
- What systems are vulnerable to security threats

IT Pro Tip

Much like a security camera that's always running "just in case," it's important to continuously review who has access to data and why, to ensure sensitive data is only available to those who should see it. This addresses both security and compliance concerns.

POST-MIGRATION: DETECT AND ALERT



2 Detect and Alert

Real-time identification of suspicious activities in your hybrid AD environment is key to minimizing the impact of an insider attack or data breach. Proactive security measures should allow you to correlate disparate IT data from numerous systems and devices to quickly detect:

- Irregular user entitlements and activity
- Any suspicious privileged account activities
- Changes that could indicate a significant insider threat
- Quick indication of an intrusion
- Whether a brute-force attack is in progress

It's also a good idea to consider solutions that improve upon native auditing tools. Native AD, Azure AD and Office 365 auditing tools lack the governance and visibility required to meet compliance regulations. There are many functional issues, including:

- Difficulty configuring auditing
- Having to configure one mailbox/object at a time
- Inability to monitor audit policies if they change or are disabled by other administrators
- Inability to automatically configure new mailboxes/objects with the desired audit policy
- Absence of real-time alerting, with only a finite number of alert actions
- Limited retention time of audited data before it is permanently lost
- Difficulty interpreting events

POST-MIGRATION: REMEDIATE AND MITIGATE

3 Remediate and Mitigate

If a breach occurs—or an access mistake is made—you need to know where problems that deviate from normal behavior exist and correct them immediately. Having a reporting process that allows you to detail everything that happens across the lifecycle will position you to act fast.

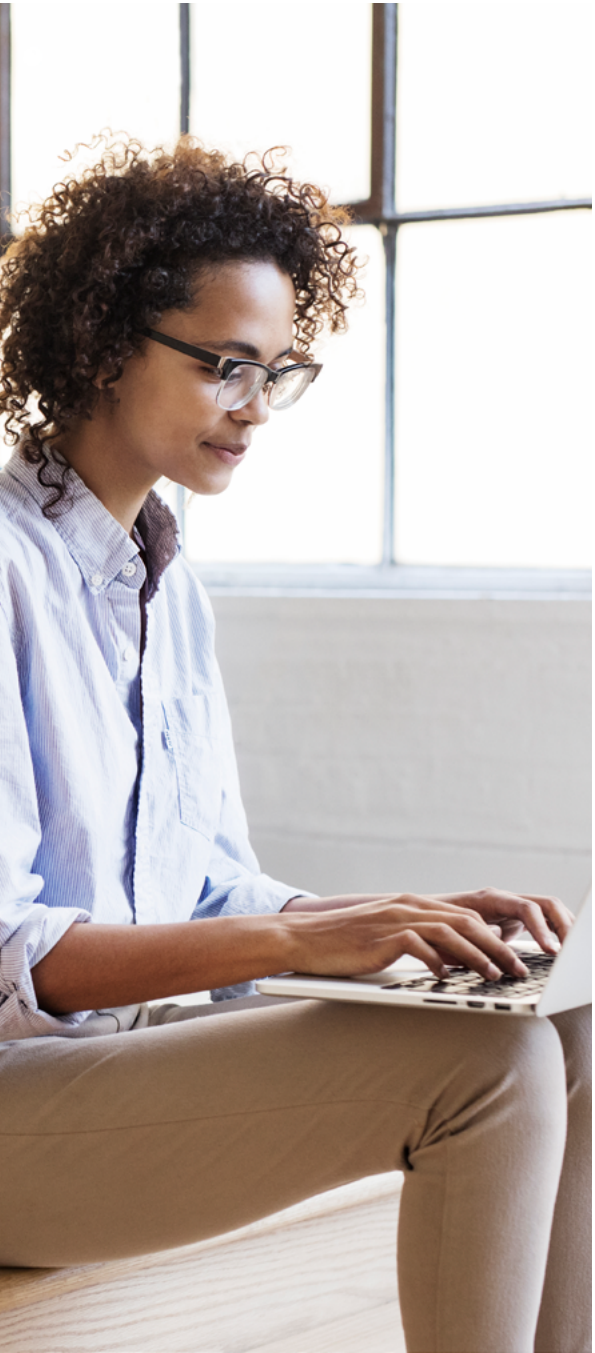
Automated security policy enforcement across your hybrid AD environment reduces the risk of human error and mitigates the potential for recurrence. The process should ensure:

- Access controls will allow whitelisted users in and keep blacklisted users out
- Users have the lowest level of user rights possible to do their jobs
- Sensitive resources are protected
- Quick, manual remediation of unauthorized changes are possible

IT Pro Tip

Common mistakes by staffers can put data at risk. Offer comprehensive training for business users that covers best practices for sharing data inside and outside the organization. The training should be reviewed annually to ensure best practices are up to date with changing technology.

POST-MIGRATION: INVESTIGATE AND RECOVER



4 Investigate and Recover

Should a security incident occur, you have to recover quickly to minimize downtime and loss of productivity. This process should allow you to analyze security baseline information so you can understand how the incident occurred and why. This process should help you to:

- Prevent a repeat incident
- Create a system for testing the business continuity plan without going off line
- Determine how long manually recover from an AD security incident will take
- Devise the best method for returning the AD to operation

HOW CAN QUEST SOFTWARE HELP?

Quest's solutions can help simplify the migration, security and management of your Office 365, Azure AD and hybrid AD environment with a world-class network of experts and partners. With its distinguished track record of delivering migration and consolidation projects and end-to-end portfolio of solutions, Quest can help you to:

- Modernize your AD to ensure cloud readiness
- Slash migration and deployment time
- Protect against security breaches
- Mitigate compliance risks
- Automate back-up and recovery
- Optimize license costs to maximize ROI

With nearly two decades of Microsoft platform migration experience, Quest enables organizations to embrace Office 365 and Azure AD without the burden of crippling costs, risks, fear or uncertainty. Learn more about how Quest can **position your hybrid environment for success**.

Quest

Join the Innovation.