Elmdale
IT Services
Ltd

6 Reasons for Microsoft Entra ID Backup

Introduction

Microsoft Entra ID (formerly Azure Active Directory) plays a critical role in modern identity and access management (IAM). However, its importance also makes it a top target for cybercriminals. With an overwhelming 600 million attacks targeting Microsoft Entra ID every day, the risks have grown increasingly complex and damaging, posing significant challenges for organisations worldwide.

The threats are as varied as they are dangerous. From phishing scams that trick users into handing over credentials to credential stuffing attacks that exploit stolen data, threat actors are relentless. The fallout is catastrophic:

- Employees lose access to critical systems, grinding productivity to a halt.
- Customers can’t access services, leading to frustration and potential churn.
- Downtime and recovery efforts drain resources, while regulatory fines add to the burden.
- News of a breach spreads quickly, eroding trust with customers, partners, and stakeholders.
- Data breaches often lead to violations of regulations like GDPR or HIPAA, resulting in hefty penalties.

Elmdale IT Services Ltd

veeam

Recovering from an attack is no small feat. It demands time, resources, and a clear strategy to restore operations and rebuild confidence. And while Microsoft provides robust security features, the onus is on organisations to protect their data according to the shared responsibility model. Security threats are just one reason you need to protect Microsoft Entra ID data, and this e-book will uncover and explain many more.

1

Security Threats

The ever-present risk of cyberattacks requires robust defenses to protect against unauthorised access and potential breaches.

2

Compliance

Proper data management practices ensure compliance with local, national, and global standards.

3

Accidental Deletions and Misconfigurations

Human error can lead to massive data loss and significant disruptions.

4

Recycle Bin Limitations

Reliance on built-in tools like the Recycle Bin is insufficient for complete data recovery.

5

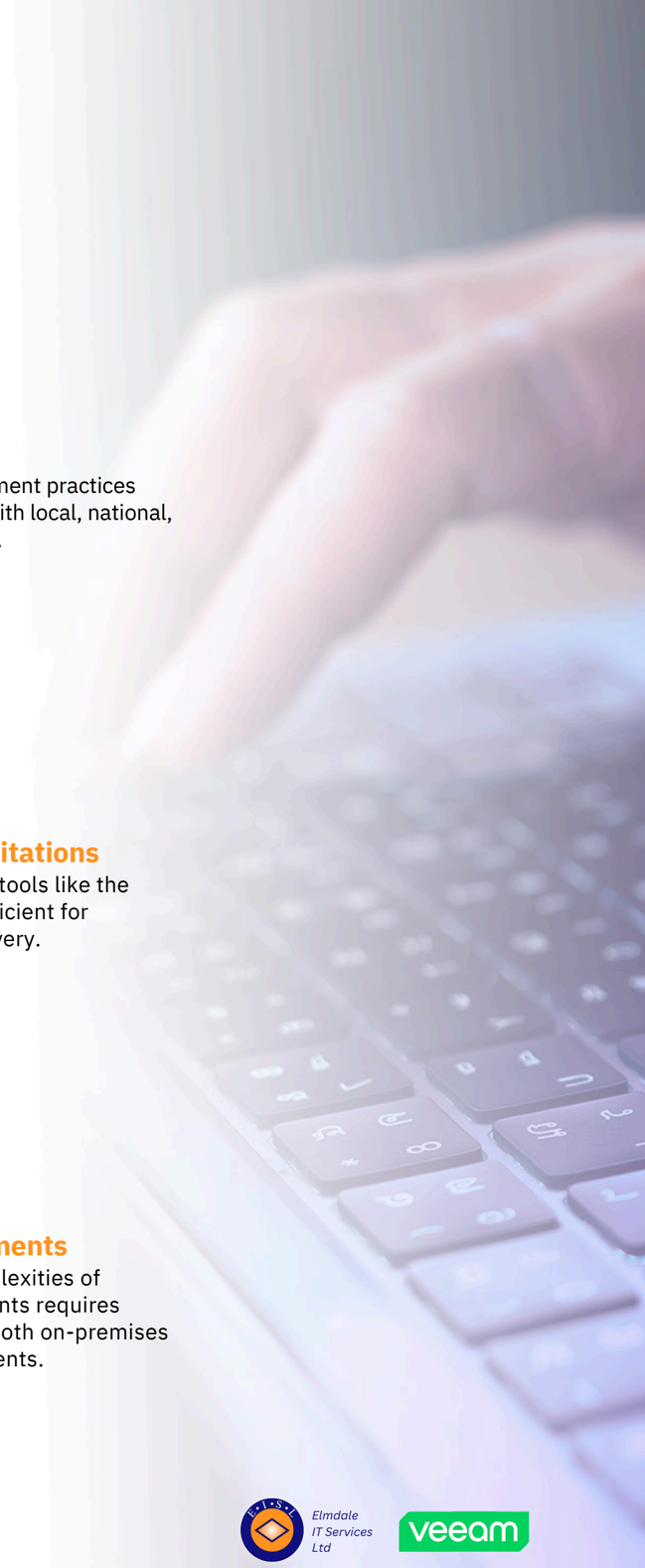
Efficient Recovery

Minimising downtime and ensuring quick recovery from data loss incidents are vital to maintaining business operations.

6

Hybrid Environments

Navigating the complexities of hybrid IT environments requires accommodates for both on-premises and cloud environments.



Elmdale IT Services Ltd

veeam

1. Security Threats

Microsoft Entra ID is integral to identity and access management (IAM) across Microsoft 365, Azure, and numerous other platforms. Often unnoticed by users, its use is crucial every time they log in. Yet, it is precisely this invisibility that makes Microsoft Entra ID a prime target for cybercriminals.

Threat actors are constantly evolving their tactics, and they only need to succeed once, while defenders must be perfect every time. Attackers are adept, employing tactics like phishing and credential stuffing, where stolen passwords are used to breach accounts. Ransomware, while different, is equally disruptive, locking organisations out of their cloud environments and halting operations.

In an ideal world, organisations would opt to prevent breaches from occurring in the first place. Many risk-mitigation strategies are very effective, and resources such as proactive monitoring and threat analysis tools help immensely.

However, no defense is foolproof. This is where backup and recovery become essential. A robust backup strategy ensures that even if attackers breach your defenses, you can quickly restore access to critical identity data. Whether it's recovering from ransomware, reversing accidental deletions, or mitigating insider threats, backups act as your safety net.

For Microsoft Entra ID, redundancy doesn't mean overkill — it means survival. When identity data is backed up and easily recoverable, organisations protect themselves against the crippling effects of losing that data.

2. Compliance

Regulatory compliance is imperative for most businesses since laws like GDPR and HIPAA demand strict adherence to data privacy, security, and transparency. The stakes are high: non-compliance can result in penalties of up to 4% of annual revenue or €20 million, whichever is greater.

In the context of Microsoft Entra ID, compliance hinges on proper management of user and group permissions. Misconfigurations or unauthorised changes can expose sensitive data, leading to breaches and compliance violations. For example, if an admin accidentally grants excessive permissions or deletes a critical user group, sensitive data could fall into the wrong hands, and regulators won't hesitate to act.

To stay compliant, organisations need robust security controls, including encryption, access management, and audit logging. But one of the most critical tools in your compliance toolkit is a comprehensive backup solution.

Backups ensure that your Microsoft Entra ID data is always secure, recoverable, and aligned with regulatory standards. If a misconfiguration or unauthorised change occurs, you can quickly detect that and restore the correct settings, minimising the risk of non-compliance and data exposure.

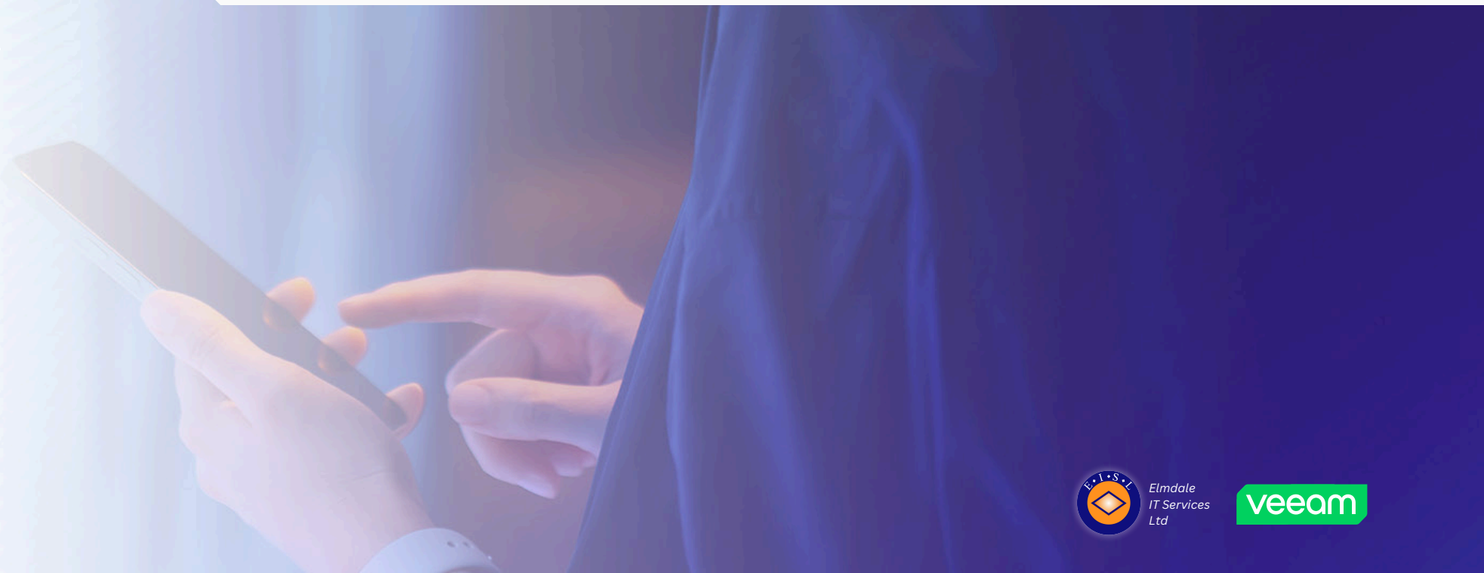
3. Accidental Deletions & Misconfigurations

Imagine if an administrator accidentally deletes a critical user group or misconfigures access controls in Microsoft Entra ID. Suddenly, legitimate users are locked out of essential systems, or worse, unauthorised users gain access. In a system as central as Microsoft Entra ID, even a small mistake can have far-reaching consequences.

The repercussions of these misconfigurations and deletions are profound. They can render critical systems inaccessible, causing operational downtime, productivity losses, and necessitating costly recovery processes. Moreover, these errors can damage the trust that customers and partners place in an organisation, potentially affecting long-term business relationships.

But here's the good news: A comprehensive backup solution can turn disaster into a minor hiccup. With backups, accidental deletions or misconfigurations can be corrected in minutes. Whether it's restoring a deleted user group or reverting to a secure, pre-error configuration, proper backups ensure that mistakes don't spiral into crises.

Mistakes will happen; it's human nature. But with a robust backup strategy, their consequences are more preventable than ever.



Elmdale IT Services Ltd

veeam

4. Recycle Bin Limitations

Alongside its short retention timeline, Microsoft EntraID's native Recycle Bin is limited in scope. Data types like Role Assignments and Conditional Access Policies are not retained at all — becoming immediately inaccessible upon deletion, meaning no second chances. Constraints on the volume of recoverable data, too, present limitations. Microsoft Entra ID's Recycle Bin is a helpful feature, but it's far from a complete solution. While it offers a recovery window of up to 30 days for certain types of data, this falls short in real-world scenarios. According to the Microsoft Defense Report 2024, the average detection time for incidents is 207 days, far beyond the Recycle Bin's retention period. By the time you realise data is missing, it's often too late to recover.

The recycle bin's story is this: Once the retention period expires or if data bypasses the recycle bin due to manual deletions or permanent removal, recovery through Microsoft's native tools becomes impossible. A dedicated backup solution is the only way to bridge these gaps and extend beyond Microsoft's built-in safeguards. Doing provides a reliable safety net against accidental or intentional data loss and ensures that nearly all types of identity data are recoverable.

5. Efficient Recovery

Breachesdon’t alwaysstart with a bang. Many begin with small, unnoticed changes — an unauthorised adjustment to permissions, the deletion of a security group, or a minor tweak in settings. The ability to detect these changes early is vital to preventing them from escalating into serious threats.

The key to preventing these issues is accelerated change detection. Administrators must be able to anticipate and address issues before they necessitate a major response. In tandem, granular recovery options empower organisations to restore exactly the objects that are needed, from a single user account to an entire directory structure, efficiently and without inducing unnecessary downtime.

So, what does efficient recovery look like for Microsoft Entra ID?
It’s a combination of:

- **Metadata Comparison:** Before restoring, compare production configurations to backup restore points. This step ensures you identify exactly what’s changed so you can restore only what’s necessary.
- **Object-Level Restore:** With granular, object-level restore capabilities, you recover specific items without disrupting the rest of your environment.

can

- **Regular Backups:** Ensure all changes and configurations are periodically saved to a secure repository. This creates a reliable safety net, enabling quick and accurate restoration when issues arise.
- **Actionable Recovery Plans:** Provide clear, step-by-step processes for restoring systems so your organisation can have a swift, secure, and seamless recovery.

Together, these elements form a comprehensive recovery strategy that minimises downtime, reduces risk, and keeps your Microsoft Entra ID environment secure and accessible.

Elmdale IT Services Ltd

veeam

6. Hybrid Environments

Managing identity across on-premises Active Directory (AD) and Microsoft Entra ID in a hybrid environment brings both flexibility and complexity. With users constantly syncing between cloud and on-prem systems, accidental deletions, misconfigurations, or synchronisation issues can disrupt access and introduce security risks. When a user is removed — either intentionally or by mistake — the ability to restore not just their identity, but also their relationships and permissions, is crucial for business continuity.

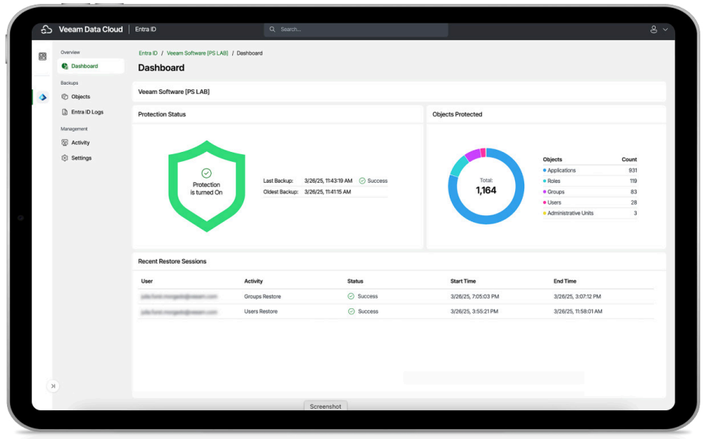
Microsoft Entra Connect and other synchronisation tools focus on keeping identity data consistent between AD and Entra ID, but they aren't designed for full recovery. When a synchronised user is deleted, Entra Connect may restore them without their original roles, group memberships, and licenses, forcing administrators to manually reconstruct their identity. This process is time-consuming and increases the risk of incomplete restorations or privilege misalignment.

Hybrid identity management isn't just about keeping users active — it's about restoring them with the right access, roles, and security settings intact. Without a proper backup strategy, IT teams may spend hours manually fixing access issues after a deletion or synchronisation mishap.

Veeam Data Cloud for Microsoft Entra ID

The challenges of securing Microsoft Entra ID are clear: human error, cyber threats, and compliance demands create constant risks. Without a resilient backup strategy, even a small misstep can lead to downtime, lost productivity, and security breaches.

Microsoft Entra ID is the backbone of your organisation's digital identity, and its protection is non-negotiable. With **Veeam Data Cloud for Microsoft Entra ID**, you can simplify data protection and ensure your identity infrastructure remains secure, compliant, and always available.



This SaaS backup solution offers:

Comprehensive Backup and Restore: Protect users, groups, application registrations, and several other objects

Unlimited Storage: Scale effortlessly with unlimited storage built-in to the SaaS backup solution

Seamless User Experience: A modern, unified UI designed for ease of use.

Microsoft Entra ID is too critical to leave unprotected. The risks are real, but so is the solution. Veeam delivers the security, resilience, and peace of mind that modern organisations need to keep their identity infrastructure protected, compliant, and always available.

Elmdale IT Services Ltd

0118 982 1444

Request a demo