

EXPOSÉ : LES VULNÉRABILITÉS D'ACTIVE DIRECTORY + LA SOLUTION DE RÉSILIENCE IDENTITAIRE



LA DURE RÉALITÉ DES ATTAQUES SUR L'INFRASTRUCTURE D'IDENTITÉ

Les vulnérabilités d'Active Directory (AD) et d'Entra ID laissent l'infrastructure d'identité de votre organisation grande ouverte aux attaques. Lorsqu'elles sont exploitées, ces failles permettent aux cybercriminels de compromettre les comptes, d'imiter les utilisateurs et de se déplacer sans être détectés dans les systèmes — compromettant ainsi toute votre stratégie de résilience identitaire.

50%

des organisations ont subi une attaque sur AD/Entra ID au cours des 1 à 2 dernières années.¹

40%

des organisations ayant subi une attaque sur AD/Entra ID ont indiqué que cette attaque avait réussi.¹

75%

des organisations feront face à une ou plusieurs attaques par ransomware d'ici 2026.²

LES VULNÉRABILITÉS QUI PERMETTENT LES ATTAQUES

La complexité d'AD le rend particulièrement vulnérable, avec plusieurs et faiblesses courantes, notamment:



Lisibilité par tous

Tout utilisateur authentifié peut lire l'intégralité de l'AD, ce qui permet aux attaquants d'exploiter des failles telles que des erreurs de configuration et des comptes privilégiés.



Confiance inhérente

Chaque système joint au domaine fait confiance à l'annuaire et est soumis à tout objet de stratégie de groupe (GPO) qui lui est appliqué.



Identifiants mis en cache

Les attaquants peuvent extraire les identifiants AD depuis n'importe quel système connecté au réseau, y compris les comptes de service privilégiés.



Objets de stratégie de groupe (GPO)

Lorsqu'ils sont liés à la tête de domaine, ils peuvent être utilisés pour désactiver des contrôles de sécurité.



Protocoles obsolètes

Les anciens protocoles, souvent laissés activés pour prendre en charge certaines applications, offrent un accès facile aux attaquants.



Paramètres par défaut

Les configurations par défaut, comme le fait d'autoriser tout utilisateur de domaine à ajouter des postes de travail, peuvent être facilement exploitées.

88%

des clients touchés par des incidents avaient une configuration AD « non sécurisée », selon le Microsoft Digital Defense Report.³



CONSEILS RAPIDES POUR LA SÉCURITÉ D'AD

Ne pas protéger AD permet aux attaquants de contrôler et de bloquer l'accès aux actifs critiques de l'entreprise à partir d'un point centralisé. Voici quelques mesures immédiates à adopter pour sécuriser AD:

01

Appliquer le principe du moindre privilège

Limitez les autorisations des comptes utilisateurs à ce qui est strictement nécessaire pour leurs tâches, réduisant ainsi le risque d'accès non autorisé.

02

Surveiller et auditer les changements

Suivez toutes les modifications apportées à AD afin de détecter rapidement toute modification non autorisée ou erreur de configuration.

03

Renforcer les configurations par défaut

Passez en revue et modifiez les paramètres par défaut d'AD. Testez soigneusement pour vous assurer que les applications existantes ne sont pas impactées.

04

Mettre en œuvre une sauvegarde et une récupération AD

Sauvegardez régulièrement les données d'AD pour disposer d'un point de restauration fiable. Des sauvegardes automatisées et fréquentes réduisent les pertes de données et le temps d'indisponibilité.

05

Désactiver les comptes inactifs

Identifiez et supprimez régulièrement les comptes utilisateurs inactifs, susceptibles d'être exploités par des acteurs malveillants.

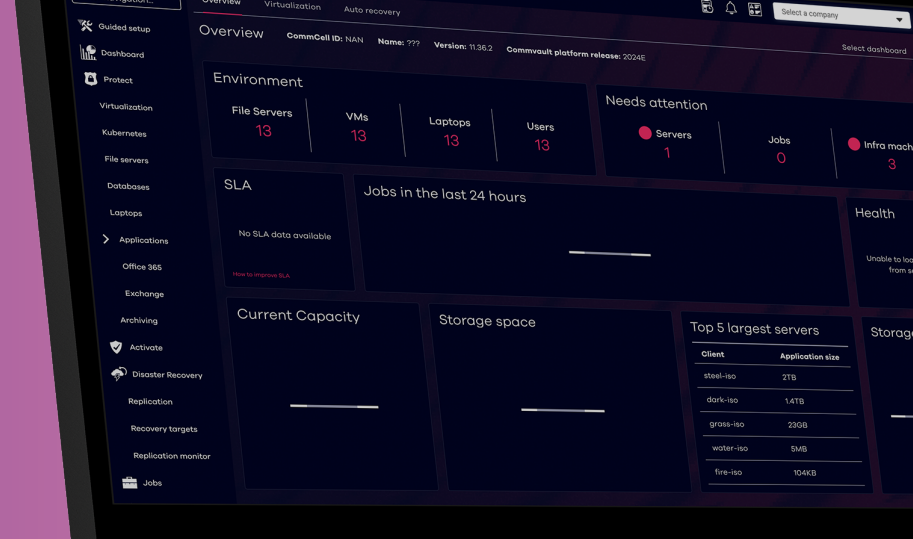
06

Préparer un plan de reprise après sinistre

Élaborez des scénarios de reprise et testez-les régulièrement pour être prêt à toute éventualité.

Commvault® Cloud pour la résilience d'active directory

Construire une résilience identitaire peut sembler complexe, mais vous n'avez pas à le faire seul. Commvault Cloud offre la protection complète nécessaire pour transformer une infrastructure AD vulnérable en une base d'identité résiliente — protégeant contre la corruption, la suppression accidentelle et les attaques malveillantes, le tout dans une solution unifiée.



En savoir plus sur la façon dont Commvault peut vous aider à protéger vos actifs critiques et à obtenir une démonstration de Commvault Cloud Backup & Recovery for Active Directory.

¹ Security Solutions, Research Finds Attackers Targeting Active Directory: 50% of Businesses Experienced an Attack with >40% Success, October 2021
² Gartner Webinar, Survive Ransomware & Build a Resistant Security Architecture
³ Microsoft Digital Defense Report 2022
⁴ Forbes, Understanding The Implications Of Active Directory Outages—And How To Fight Back, September 2024
⁵ SC Media, Organizations prioritize ITDR solutions that protect Active Directory before, during, and after a cyberattack, April 2023