eBOOK

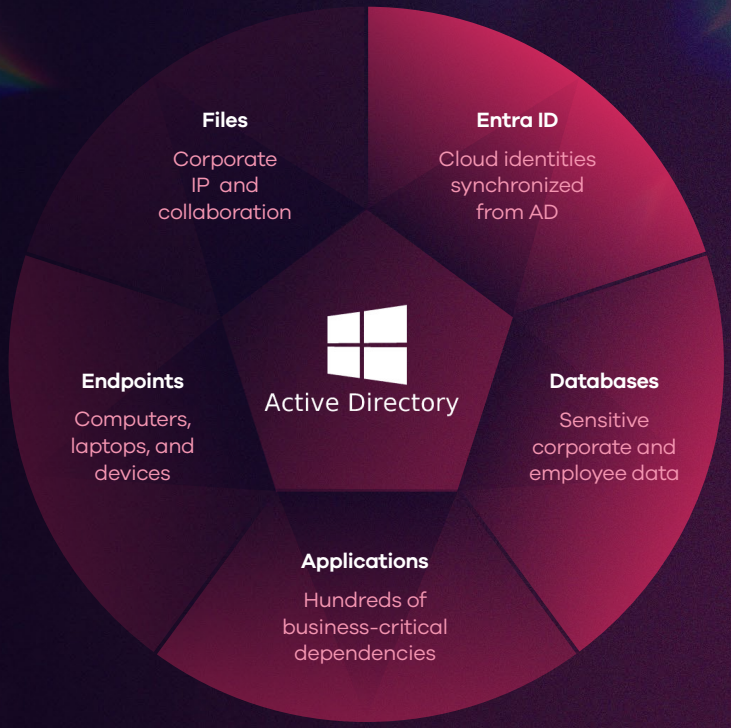
PROTEGGI I

Pietre della Corona

Sicurezza di
Active Directory contro
le Minacce Cibernetiche

Commvault®

L'Importanza e la Complessità di Active Directory



Microsoft Active Directory (AD) e Entra ID sono le fondamenta della gestione delle identità e degli accessi aziendali, autenticando milioni di utenti a livello globale e controllando l'accesso ai sistemi aziendali critici. Dalle autenticazioni delle workstation all'accesso fisico agli edifici, AD consente l'operatività fluida della tua organizzazione.

Se i dati di AD si corrompono o la directory stessa diventa non disponibile, ciò può causare un grave disguido nelle applicazioni e processi di business, bloccando l'accesso degli utenti ai sistemi e risorse vitali.

Senza AD, le operazioni aziendali si fermano.

Il personale bancario non può accedere agli account dei clienti.

I medici e le infermiere non possono accedere ai record medici.

I programmatori non possono pubblicare codice.

I manager non possono inviare email.

I diversi team non possono collaborare o chattare.

L'Importanza e la Complessità di Active Directory lo Rendono un Obiettivo Primario per gli Attaccanti.

Poiché AD e la gestione delle identità sono componenti cruciali delle operazioni aziendali, rappresentano un obiettivo molto attraente per gli attaccanti che cercano sistemi preziosi da tenere in ostaggio. Per coloro che desiderano semplicemente causare caos, AD è uno dei sistemi che può portare tutti gli altri a un arresto e devastare l'azienda.

AD è il centro dell'autenticazione sicura e dei servizi, e mantenere la sua sicurezza e recuperabilità è critico, preparandosi alle varie catastrofi che potrebbero colpirlo.

AD è coinvolto in circa il

90%

degli attacchi.[1]

Data la sua importanza, non sorprende che

I report della Microsoft Digital Defense indicano che il

88%

dei clienti

colpiti da incidenti di sicurezza aveva una configurazione AD non sicura, rendendo AD un bene di alto valore che i malintenzionati sono ansiosi di sfruttare.[2]

Per gli attaccanti, AD è un punto di riferimento per acquisire privilegi elevati e rubare, corrompere o negare l'accesso ad applicazioni e dati critici.

Un recente rapporto di IBM evidenzia un aumento del **100%** degli attacchi "kerberoasting",

dove gli attaccanti cercano di ottenere privilegi elevati sfruttando Microsoft AD.[3]

1 Researchers Explore Active Directory Attack Vectors
2 Microsoft Digital Defense Report 2022
3 IBM Report: Identity Comes Under Attack Straining Enterprises' Recovery Time from Breaches

Il recovery dell'AD è il fondamento della continuità operativa aziendale

L'importanza di prioritizzare il ripristino di AD diventa evidente quando si considera il suo effetto a cascata su altri carichi di lavoro. Applicazioni, file systems, servizi di posta elettronica e database dipendono tutti da AD per l'autenticazione corretta e l'accesso degli utenti. Quando AD è danneggiato o completamente offline, le applicazioni e i servizi critici diventano inaccessibili.

Poiché quasi tutto nelle moderne aziende dipende dall'identità, il ripristino di AD prima di altri carichi di lavoro è una priorità critica.

Ripristinando AD per primo, le organizzazioni possono ri-stabilire il controllo sulle loro reti e sistemi, verificare che le politiche di sicurezza dei dati e di accesso siano applicate e fornire una base stabile per il ripristino di altri sistemi e servizi.

GLI ERRORI SUCCEDONO:

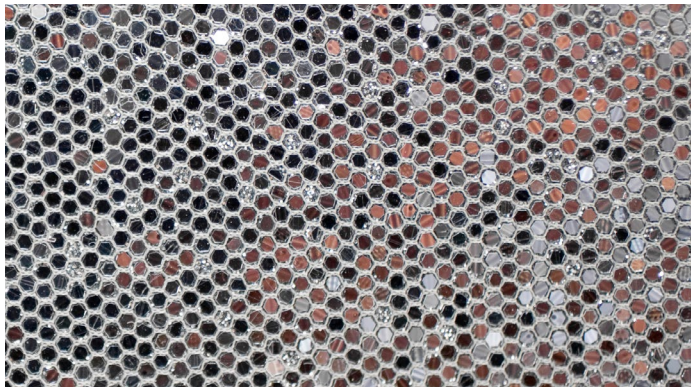
La Necessità di un Ripristino Granulare

Uno degli aspetti più critici della protezione di AD è la capacità di ripristinare rapidamente i dati persi o corrotti. Quando dati importanti all'interno di AD vengono accidentalmente o maliziosamente eliminati, modificati o corrotti, è necessario poter identificare rapidamente queste modifiche e ripristinare singoli oggetti e attributi.

Sebbene sia utile che il Cestino (Recycle Bin) in AD possa ripristinare temporaneamente gli oggetti eliminati, fare affidamento su questo metodo è rischioso. Il Cestino mantiene gli oggetti eliminati per un periodo limitato prima di rimuoverli definitivamente. Non supporta il rollback delle modifiche a livello di attributo o la reversibilità delle modifiche ai Group Policy Objects (GPO) o alle configurazioni di AD.

A volte, le catastrofi possono non portare all'eliminazione degli oggetti, ma piuttosto alla Sovrascrittura dei dati degli attributi su più oggetti. Ad esempio, uno script PowerShell mal scritto potrebbe causare modifiche inaspettate in tutta la directory. Quando ciò accade, è necessario avere la capacità di localizzare e annullare specifici attributi su più oggetti all'interno di AD. Tuttavia, il Cestino non può annullare le modifiche a livello di attributo o ripristinare le modifiche ai GPO o alle configurazioni di AD.

Per una protezione completa, è meglio avere un backup completo e frequente di tutta l'AD. Una soluzione dedicata per la protezione dei dati consente il ripristino granulare, ripristinando solo l'attributo dell'oggetto mancante, danneggiato o mal configurato. Questa granularità può riportare rapidamente online i sistemi aziendali o gli utenti senza la necessità di un ripristino completo di un intero ambiente AD.



Hai un Piano di Ripristino?

Quando il ransomware blocca e mette offline i server che ospitano il tuo AD, è necessario avere la capacità di ripristinare l'intero ambiente. Questo implica la ricostruzione del servizio di directory, inclusi domini, controller di dominio e dati associati, a uno stato pre-attacco.

L'impatto di un attacco che disabilita i controller di dominio è reale e può essere devastante. I sistemi critici smettono di funzionare. Gli impiegati non possono accedere. Le politiche di sicurezza basate sull'identità non possono essere applicate.

"Se non possiamo ripristinare i nostri controller di dominio, non possiamo ripristinare nulla"

AMMINISTRATORE IT, MAERSK

Con minacce del genere in agguato, avere un piano di ripristino ben documentato e frequentemente testato per ricostruire e ripristinare il tuo ambiente AD ad uno stato precedente e sano pre-attacco è critico e la chiave per riprendere rapidamente le attività aziendali.

Ransomware Attacca

Nel 2017, il gigante globale delle spedizioni Maersk è caduto vittima dell'attacco cibernetico NotPetya, che ha cifrato file systems di

45.000
PC

4.000
servers

150
e quasi tutti i controller di dominio AD

Con AD completamente offline, le operazioni si sono interrotte immediatamente, chiudendo

17
porti di spedizione globali e bloccando

100s
di navi container per **10 giorni.**

In totale, l'attacco è costato alla società almeno

300
milioni di dollari

4 The Untold Story of NotPetya, the Most Devastating Cyberattack in History

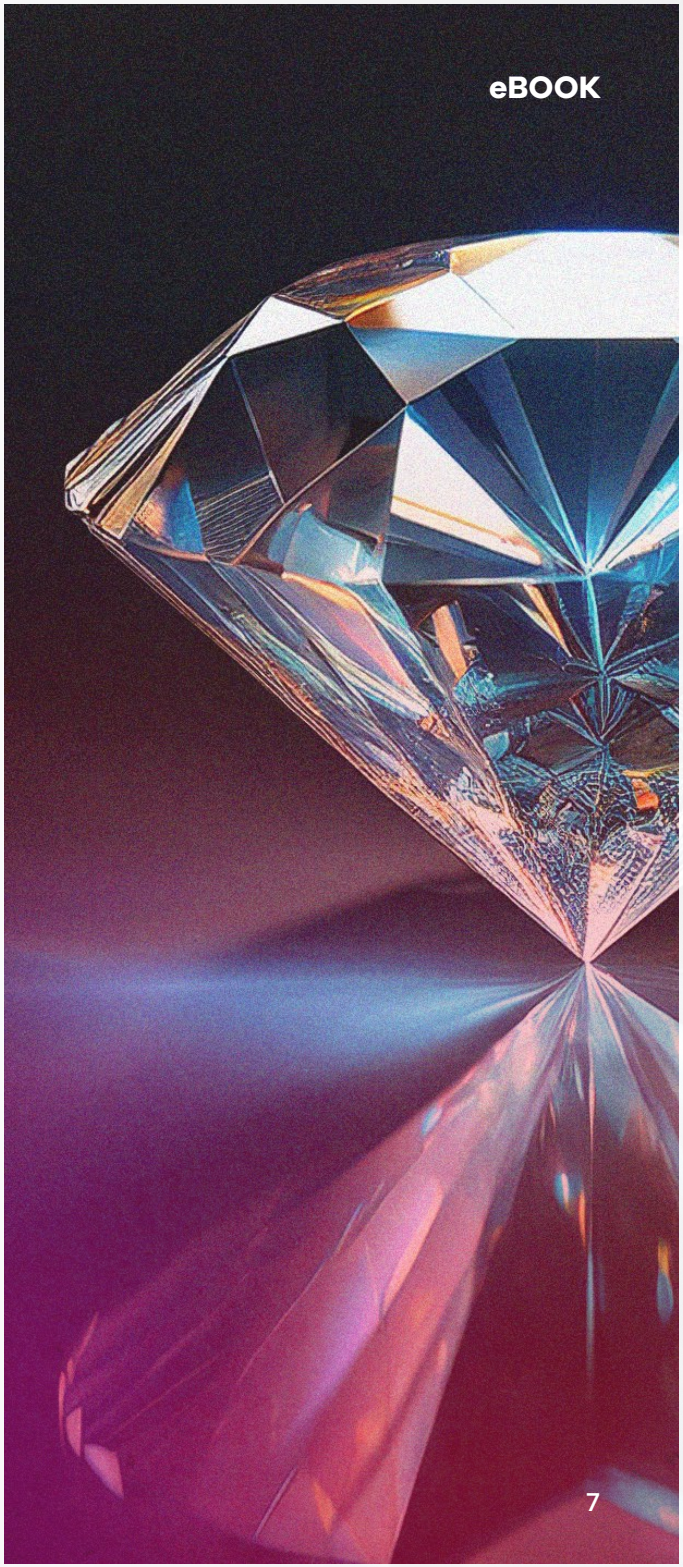
Ripristino di Active Directory: Un Compito Complesso

Le foreste AD sono ambienti complessi con più domini, diversi controller di dominio per ciascuno di questi domini e una gerarchia completa di utenti, computer e impostazioni di accesso/sicurezza. In caso di un attacco cibernetico, non basta semplicemente ripristinare un singolo controller di dominio da backup. Il processo di ripristino e ricostruzione dell'ambiente è incredibilmente intricato e richiede una coordinazione meticolosa. Ogni controller di dominio deve essere sincronizzato e ripristinato con cura per evitare incongruenze dei dati e potenziali corruzioni.

La Guida al Ripristino della Foresta AD di Microsoft fornisce un metodo dettagliato e passo-passo per questo, che può coinvolgere da 50 a 100 o più passaggi individuali, a seconda della dimensione della tua organizzazione.

Il processo di ripristino è manuale, lungo e complesso – spesso richiede giorni o settimane per completarsi. Nel frattempo, le operazioni aziendali cessano di funzionare e gli utenti non possono accedere alle applicazioni importanti.

Senza automatizzare e orchestrare il processo, si rischia di ripristinare AD in uno stato non utilizzabile, il che potrebbe ulteriormente interrompere le attività aziendali e prolungare l'interruzione.



Commvault Rende la tua Active Directory Resiliente

Commvault Cloud Backup & Recovery for Active Directory ti permette di proteggere e accelerare il ripristino di AD in caso di corruzione, eliminazione accidentale e attacchi ransomware.

Accelerare il ripristino di AD e tornare più rapidamente agli affari con:

Ripristino automatico della foresta:

Ripristina rapidamente le foreste a un punto nel tempo precedente all'attacco, permettendoti di riprendere le attività aziendali in ore invece che in giorni o settimane.

Confronti interattivi:

Identifica le modifiche al dominio, permettendoti di ripristinare rapidamente gli oggetti eliminati accidentalmente o maliziosamente o di annullare gli attributi sovrascritti in tutta la directory.

Ripristino flessibile e granulare:

Ripristina rapidamente solo gli attributi degli oggetti mancanti, danneggiati o mal configurati, riportando rapidamente online i sistemi aziendali o gli utenti.

Supporto per directory ibride:

Proteggi oggetti critici di Microsoft AD e Entra ID, inclusi GPO, utenti, gruppi, policy di accesso condizionale, ruoli e altro ancora.

Test di ripristino di AD:

Fornisci la certezza che i ripristini possano essere effettuati con successo, permettendo alle squadre di sicurezza e IT di esercitarsi in tempi tranquilli per prepararsi ai momenti critici.

Il Cyber Recovery è più che solo AD

Affrontare un attacco cibernetico o una situazione di ransomware è un'esperienza terrificante.

Ripristinare AD è il primo passo in molti casi, e trovare modi per automatizzare un processo altrimenti lungo e risorse-intensivo può aiutare ad avviare rapidamente il processo di ripristino e riportare rapidamente l'operatività aziendale. Ancora meglio è quando il tuo ripristino AD si basa sulla stessa piattaforma su cui si fonda il resto del tuo ripristino cibernetico.

Unificare il processo di ripristino e ricostruzione cibernetica su una piattaforma comune abilita una coordinazione, automazione e orchestrizzazione che va oltre il semplice ripristino delle identità – puoi orchestrare il ripristino di applicazioni, dati, cloud e infrastrutture. Questo aiuterà le tue squadre a lavorare insieme per ricostruire i sistemi dopo gli attacchi cibernetici e le catastrofi, costruendo una resilienza che garantisce un'attività aziendale continua.

eBOOK

Richiedi una demo e scoprirai come ripristinare l'intera foresta AD in pochi clic per continuare a gestire il tuo business.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®