COHESITY

GUIDE D'ACHAT

UN GUIDE DES DIRIGEANTS POUR ÉVALUER LES SOLUTIONS DE RÉSILIENCE POUR L'IDENTITÉ

Tout ce que vous devez savoir pour verrouiller l'accès, protéger les données précieuses et vous remettre rapidement des cyberattaques destructrices

Vos systèmes de gestion des identités et des accès sont une cible privilégiée pour les acteurs malveillants.

Pourquoi ?

9 cyberattaques sur 10 visent des systèmes de gestion des identités et des accès (IAM). C'est la partie la plus attaquée de l'infrastructure d'une entreprise.

Un système d'identité de référence est une cible de grande valeur, car sa compromission permet aux attaquants d'accéder pratiquement à toutes les ressources de l'entreprise. C'est pourquoi la résilience de l'identité est la pierre angulaire d'une stratégie complète de cyber-résilience. Pour restaurer rapidement une entreprise opérationnelle a minima, les services d'identité doivent faire partie des premières charges de travail à rétablir à un état de confiance, car tant de systèmes et de processus métier critiques en dépendent.

Pour la plupart des entreprises, le principal IAM et la source de vérité pour les autres fournisseurs d'identité est Microsoft Active Directory (AD) en local. La cyber-restauration d'AD, en particulier dans les environnements complexes qui comprennent plusieurs forêts, est un processus difficile qui nécessite une expertise spécialisée. Il ne s'agit pas d'une « charge de travail supplémentaire ». En plus d'AD, vous avez probablement un mélange d'Entra ID et d'Okta.

Alors que vous cherchez à renforcer vos défenses contre les cyberattaques, vous devez vous assurer que vous disposez d'une stratégie de résilience de l'identité de bout en bout pour tous vos services d'identité critiques.

> ***« Aucune organisation ne peut être protégée à 100 % contre les cyberattaques. Il est donc essentiel d'investir dans la résilience, c'est-à-dire dans la capacité à se rétablir rapidement après une compromission. »***

La résilience de l'identité garantit que votre entreprise peut :

- **Détecter et remédier aux menaces d'identité :** Détectez les attaques basées sur l'identité en cours et annulez automatiquement les changements risqués qui ne peuvent pas attendre l'intervention humaine, avec la détection et la réponse aux menaces d'identité (ITDR).
- **Restaurer proprement les services d'identité et restaurer la confiance :** Restaurez vos services d'identité sans restaurer les attaquants et/ou les portes dérobées qui entraînent une réinfection persistante.
- **Réduisez les temps d'arrêt :** L'identité est essentielle pour l'accès et l'authentification. Lorsqu'elle tombe, l'entreprise s'arrête. Assurez-vous que les opérations commerciales peuvent être récupérées de manière sécurisée et transparente après une attaque visant l'identité afin de réduire les temps d'arrêt.

Aucune entreprise ne peut être 100 % à l'abri des cyberattaques – vous devez donc investir dans la résilience pour avoir la capacité de rebondir après une violation. Votre entreprise doit améliorer et étendre la résilience de l'identité en détectant et en corrigeant en permanence les attaques basées sur l'identité et en mettant en œuvre une stratégie de restauration éprouvée qui restaure AD, Entra ID et Okta proprement et rapidement en toutes circonstances. Ce guide vous aidera à évaluer les solutions, à poser les bonnes questions et à investir en toute confiance dans la sécurisation de votre infrastructure d'identité contre les menaces actuelles.

Ce qu'il faut rechercher dans une solution de résilience de l'identité

Lors de l'évaluation des options, il est tentant de considérer l'identité comme une simple charge de travail supplémentaire à sauvegarder et à restaurer si nécessaire. C'est un état d'esprit dangereusement obsolète. Une approche moderne qui étend la cyber-résilience aux systèmes d'identité et d'accès combine une sécurité proactive avancée et une restauration propre à chaque étape du cycle de vie de l'attaque. Voici ce qui sépare une véritable solution de résilience de l'identité prête pour l'entreprise des autres :

ITDR avancé : La résilience de l'identité commence avant la violation. Les systèmes IAM comme AD sont souvent les premiers systèmes ciblés par les attaquants, car ils fournissent les clés du royaume. Il ne suffit pas de les sauvegarder. Votre solution doit être en mesure de fournir une surveillance continue de la posture de sécurité de votre environnement d'identité grâce aux capacités de détection et de réponse aux menaces d'identité. Cela peut aider à détecter les vulnérabilités afin de renforcer votre infrastructure d'identité et d'automatiser la correction. La restauration et la correction automatisées des changements malveillants qui ne peuvent pas attendre l'intervention humaine peuvent réduire les risques d'une attaque réussie. En mettant en œuvre ces mesures de détection et de correction continues des menaces, ainsi qu'un renforcement proactif, vous pouvez vous assurer que les attaquants se heurtent à des obstacles avant de pouvoir militariser vos systèmes d'identité.

Une protection qui résiste aux attaques : En cas de compromission, il est important de vous assurer que votre infrastructure d'identité peut être restaurée à partir de données de sauvegarde propres. Les attaquants savent que les sauvegardes sont la dernière ligne de défense, c'est pourquoi ils s'engagent activement dans des schémas de double extorsion ou tentent de les chiffrer, de les modifier ou de les supprimer, vous laissant largement sans défense et contraint de payer des rançons exorbitantes. Votre solution de résilience de l'identité doit fournir une immuabilité par conception, garantissant que les sauvegardes AD ne peuvent pas être altérées même si les attaquants obtiennent des identifiants d'administrateur de domaine. Le stockage WORM, les approbations basées sur le quorum et la vérification cryptographique sont des capacités essentielles pour des sauvegardes résilientes. Si votre couche de protection ne résiste pas lorsque des adversaires se trouvent à l'intérieur de votre réseau, vous n'avez pas vraiment de protection.

Restauration rapide et sans logiciel malveillant : Lorsque l'identité est compromise, les temps d'arrêt s'étendent à toutes les fonctions de l'entreprise. La vitesse de restauration est importante, mais l'intégrité de la restauration aussi. Restaurer l'identité sans valider sa fiabilité risque de réintroduire des logiciels malveillants ou des portes dérobées, entraînant des infections répétées et de redoutables boucles infernales. Une solution efficace doit combiner une restauration rapide, orchestrée et automatisée d'AD, d'Entra ID et d'Okta. Pour AD en particulier, les restaurations doivent être découplées du système d'exploitation pour s'assurer que les informations d'identification compromises et les logiciels malveillants ne sont pas réintroduits. Pendant un

processus de restauration, cela peut réduire les temps d'arrêt en prévenant les infections persistantes grâce à une restauration fiable.

Options de restauration granulaire : Tous les incidents d'identité ne nécessitent pas une restauration complète. La restauration granulaire permet de gagner du temps et de réduire les perturbations en vous offrant des options de restauration au niveau de l'objet, de l'attribut et de la forêt. Disposer d'outils de restauration granulaire et forestière garantit qu'il existe une solution appropriée pour les demandes de type help-desk et les cyber-événements complets.

Protection à travers l'identité hybride : L'identité n'est plus limitée à l'AD local. Entra ID et Okta deviennent rapidement un élément crucial de l'architecture d'identité d'entreprise, en particulier pour l'accès aux applications cloud. Vous avez besoin d'une solution de résilience à l'épreuve du temps pour fonctionner de manière transparente dans les environnements d'identité hybrides, protégeant à la fois AD, Entra ID et Okta. Pour de nombreuses entreprises, Entra ID et Okta sont synchronisés avec AD, ce qui signifie que pour restaurer avec succès et en toute sécurité Entra ID et Okta, vous devez d'abord pouvoir protéger et restaurer AD. Entra ID et Okta sont des applications distinctes d'AD avec des synchronisations unidirectionnelles du site local vers le cloud. Sans la protection locale, vous n'avez que la deuxième moitié d'une solution. Votre solution de résilience d'identité doit également inclure des capacités de protection et de restauration pour garantir qu'Entra ID et Okta sont sécurisés et peuvent être restaurés proprement, afin d'assurer la continuité de l'identité cloud.

Analyses des preuves post-violation pour valider la confiance et prévenir les attaques futures : Une restauration sans visibilité vous rend vulnérable à des incidents répétés. Une solution moderne doit intégrer des capacités d'analyse médico-légale permettant aux équipes de valider une restauration saine. Cela facilite non seulement les enquêtes post-incident, mais éclaire également de manière cruciale les mesures préventives, aidant les entreprises à renforcer leurs défenses et à respecter les exigences de conformité ou de création de rapports réglementaire. Sans la diligence raisonnable après la restauration, vous risquez une attaque de suivi. L'analyse des preuves devrait être au cœur des préoccupations. C'est un élément essentiel de la résilience de l'identité.

Possibilité de restaurer sans accès à Internet : En cas de panne catastrophique ou de cyberattaque, vous ne pouvez pas supposer que vous disposerez d'un accès Internet stable ou sécurisé. Votre solution de résilience de l'identité doit être en mesure de restaurer avec succès vos systèmes d'identité critiques sans accès à Internet afin que vous puissiez effectuer une restauration saine et remettre les systèmes en ligne en toutes circonstances.

Assistance rapide en réponse aux incidents, 24 h/24 et 7 j/7 : L'identité est une charge de travail unique et complexe, en particulier lorsqu'il s'agit de la restaurer. En ce qui concerne la cyber-restauration de l'infrastructure d'identité critique, il est essentiel de s'assurer que le fournisseur de la solution dispose d'une expertise éprouvée dans la protection, la sécurisation et la restauration de l'identité et puisse fournir au client les conseils nécessaires. Chaque restauration peut varier, et le soutien approprié ainsi que les analyses de la preuve de la part de vétérans chevronnés sont essentiels pour garantir que votre entreprise puisse se restaurer des attaques d'identité ou des pannes les plus catastrophiques en toute confiance et rapidement.

Questions essentielles à poser aux fournisseurs

1. Comment empêchez-vous les pirates de falsifier ou de supprimer les sauvegardes AD, Entra ID ou Okta ?
2. Pouvez-vous démontrer la restauration complète de l'ensemble de votre infrastructure d'identité en moins d'une journée ?
3. Comment vérifiez-vous que les AD, Entra ID ou Okta récupérés sont exempts de logiciels malveillants, de portes dérobées ou n'ont pas restauré des identifiants compromis ?
4. Pouvez-vous restaurer l'identité avec la même expérience et la même interface utilisateur sans accès à Internet ?
5. Prenez-vous en charge les environnements d'identité hybrides (AD local + Entra ID + Okta) ?
6. Votre solution peut-elle exécuter des restaurations complètes de forêt pour AD de manière automatisée et respecter le Microsoft Recovery Runbook ?
7. Votre solution recherche-t-elle les menaces spécifiques à l'identité afin de détecter et d'éliminer les acteurs malveillants avant qu'une compromission ne se produise ?

Signes d'avertissement à surveiller

- Aucune capacité de sécurité de l'identité. La résilience comprend la réduction des risques avant l'impact et l'atténuation des menaces pour éviter une compromission.
- Solutions reposant uniquement sur des outils Microsoft natifs. Ils sont manuels, lents et peu fiables lorsque vous en avez le plus besoin.
- Sauvegardes stockées en production. Les attaquants peuvent les effacer et vous laisser sans rien avec quoi restaurer avec.
- Aucune orchestration ou automatisation pour les restaurations parallèles de plusieurs contrôleurs de domaine (DCs). Sans elle, cela oblige les administrateurs à suivre de longues étapes manuelles pendant une période de stress élevé et dans un environnement chaotique.
- La solution repose sur un accès Internet sécurisé et stable. Vous ne pouvez pas supposer ou vous fier à une connexion Internet pendant une cyberattaque ou une restauration.
- Aucune capacité de tester la restauration. Si vous ne pouvez pas la simuler, vous ne pouvez pas lui faire confiance.
- Pas de possibilité de découpler le système d'exploitation pendant la restauration. Ramener le système d'exploitation avec vos données d'identité peut ramener des logiciels malveillants et des portes dérobées.
- Aucune capacité à cibler une source physique/virtuelle pour la restauration. La nécessité d'un niveau exact de correctif peut entraîner des temps d'arrêt prolongés.
- Aucune expertise en analyse de preuves numériques liée à l'identité et en réponse aux incidents (IFIR) pour une prise en charge 24 h/24 et 7 j/7 de la réponse aux incidents.

Liste de contrôle d'évaluation du fournisseur

Utilisez cette fiche d'évaluation pendant vos conversations avec les fournisseurs :

Besoin	Fournisseur 1	Fournisseur 2	Fournisseur 3	Notes
Sauvegardes AD immuables et isolées				
Objection à la granularité de restauration au niveau de la forêt				
Flux de travail automatisés de restauration de forêt				
Renforcement proactif pour identifier et fermer les vecteurs d'attaque				
Détection de logiciels malveillants/corruption dans les sauvegardes				
Suivi inviolable des modifications multisources et restauration				
Inventaire et surveillance des comptes de service hautement ciblés				
Prise en charge de l'AD hybride (localement + Entra ID)				
Analyse des preuves post-violation				
Évolutivité (multi-forêts/monde)				
Assistance 24 h/24, 7 j/7 pour la réponse aux incidents liés à l'identité				
Restaure plusieurs contrôleurs de domaine (DC) en parallèle (pour AD)				
Cible toute source physique/virtuelle pour la restauration				
Restaure plusieurs contrôleurs de domaine en parallèle (pour AD)				

Conclusion

La compromission basée sur l'identité est au cœur de presque toutes les violations majeures. C'est pourquoi l'accélération de la cyber-résilience en ce qui concerne vos systèmes d'identité critiques n'est plus facultative : elle est fondamentale pour la sécurité de l'entreprise.

Une solution éprouvée de résilience de l'identité va au-delà des sauvegardes. Elle durcit l'identité contre les compromissions, protège contre les attaques et les menaces liées à l'identité, offre une restauration fiable ultra-rapide et vous aide à fermer les portes dérobées pour des restaurations fiables sans logiciels malveillants. Pour en savoir plus sur la résilience de l'identité et sur la manière dont elle pourrait vous aider à sécuriser vos services d'identité les plus critiques, parlez-en à votre équipe Cohesity en charge de votre compte dès aujourd'hui.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500064-001-FR 8-2026