CYBERARK®

EBOOK

La sécurité des identités : pourquoi est-ce important, et pourquoi maintenant ?

Éliminez les risques en adoptant une approche unifiée de la gestion des identités

Table des matières

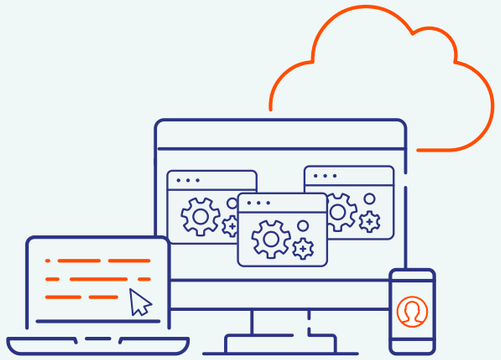
Introduction

Le message véhiculé par les malfaiteurs est très clair: toute identité est une cible.

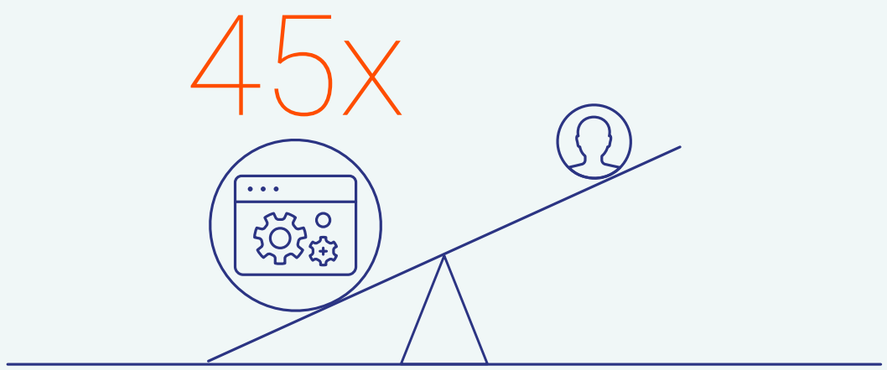
Si l'on observe le paysage de l'entreprise moderne, il est facile de comprendre pourquoi. Chaque employé a plusieurs identités et utilise plusieurs appareils. Des tiers peuvent accéder aux systèmes critiques via leurs terminaux ou applications. À cela s'ajoutent les accès à privilèges dont les identités machines ont besoin pour fonctionner, et le fait que celles-ci sont désormais 45 fois plus nombreuses que les identités humaines.[1]

Bien entendu, les identités seules ne présentent pas de risques inhérents, pourvu qu'elles soient correctement gérées et sécurisées. Mais les initiatives transformatrices des entreprises, en particulier la migration vers le Cloud, l'essor du télétravail, l'automatisation et le DevOps, ont entraîné une multiplication des identités avec des accès sans précédent, faisant de toute identité une cible de choix. Dans les environnements multiClouds, il n'est pas rare que les identités reçoivent un dangereux mélange de droits, ce qui élargit davantage la surface d'attaques que les équipes de sécurité doivent protéger.

[1] CyberArk « 2022 Identity Security Threat Landscape Report », avril 2022



En moyenne, un employé a accès à plus de 30 applications et comptes



Les identités machines sont 45 fois plus nombreuses que les identités humaines

Source: CyberArk « 2022 Identity Security Threat Landscape Report » (n=1750)

La prolifération des identités : une menace croissante

Au vu de la situation, il n'est pas étonnant que 80 % des violations soient dues à des identifiants compromis.[2] Les experts informatiques et de la sécurité ne connaissent que trop bien ce problème, et ont conscience de la prolifération des identités découlant des initiatives de transformation numérique menées par les entreprises. En outre, 98 % des spécialistes en matière d'identité et de sécurité ont déclaré que l'augmentation du nombre d'identités était engendrée par l'adoption du cloud, l'établissement de relations avec des tiers et les identités machines.[3]

Les initiatives de transformation numérique peuvent aller à l'encontre de la gestion des identités. Il est difficile de trouver le bon équilibre entre vitesse et sécurité dans un monde où l'entreprise forme désormais un réseau complexe de terminaux physiques et virtuels, d'appareils, de flux de travail dans le Cloud et de solutions SaaS.

Demander aux utilisateurs de s'authentifier de manière répétée aux systèmes et aux applications, et de tenir à jour plusieurs mots de passe complexes, peut se révéler fastidieux et chronophage. Après tout, les choses évoluent rapidement dans cet environnement. Mais il en va de même pour les attaquants, qui appliquent toujours le même mode opératoire: trouver une identité qui n'a pas été protégée par des contrôles intelligents des privilèges et l'exploiter à des fins malveillantes. Alors que les entreprises sont de plus en plus nombreuses à passer à un environnement hybride ou multiCloud, les attaquants peuvent utiliser encore plus de failles (dans ce cas, les identités) comme points d'entrée.

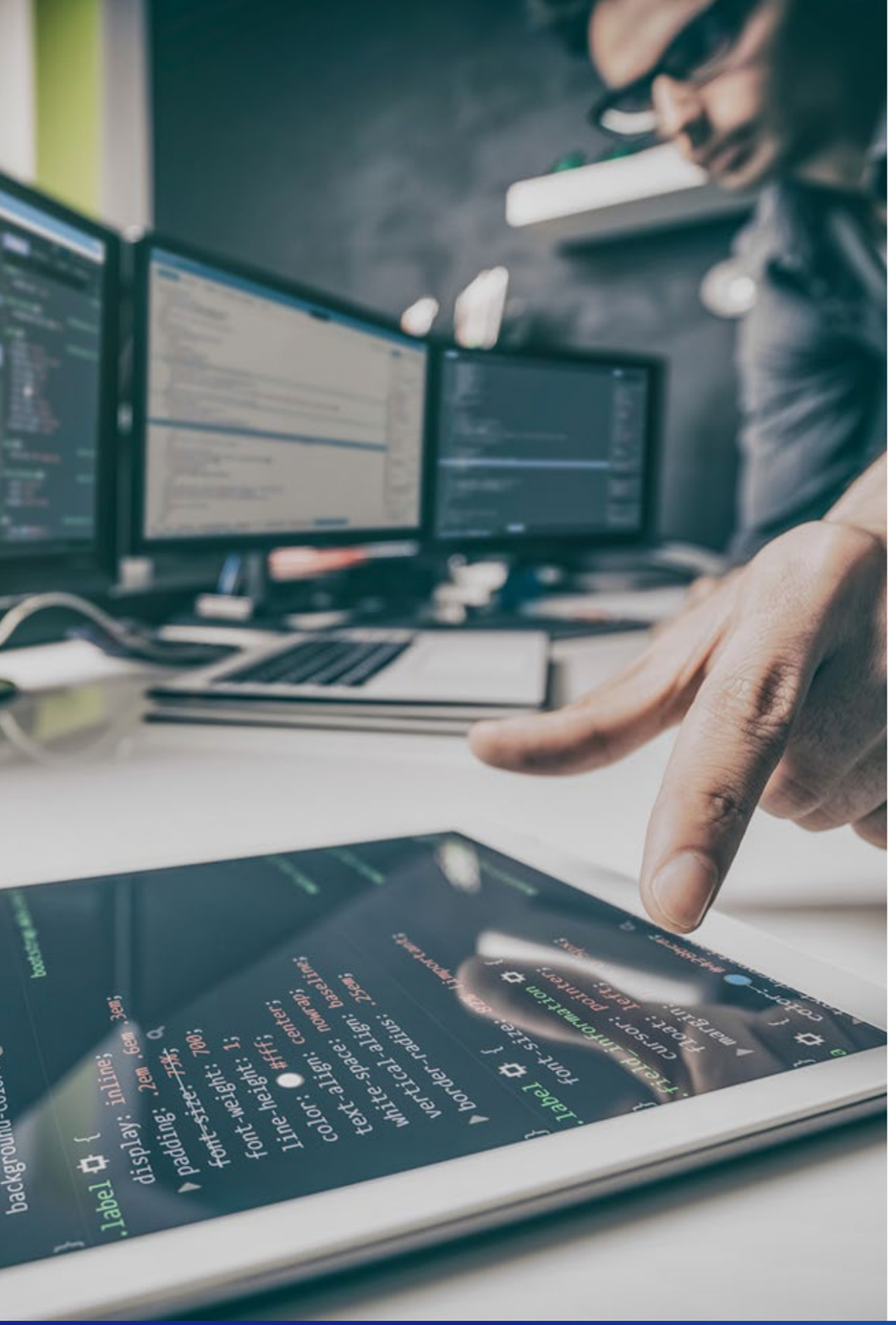
En résumé, les entreprises sont comme qui dirait coincées entre le marteau et l'enclume, entre la nécessité de sécuriser du mieux possible tous les systèmes et toutes les données et la nécessité de maintenir la productivité des équipes, et les malfaiteurs en profitent.

[2] Verizon Data Breach Investigations Report, mai 2022
[3] Identity Defined Security Alliance, 2022 Trends in Securing Digital Identities, juin 2022

Le problème des solutions traditionnelles de gestion des accès

L'identité représente le nouveau domaine dans lequel les entreprises luttent contre les menaces émergentes à mesure que la surface d'attaques s'agrandit. Les solutions traditionnelles de gestion des identités et des accès (IAM) n'ont pas été conçues comme un outil défensif pour gérer la prolifération des identités à laquelle les équipes de sécurité sont actuellement confrontées. Elles n'étaient pas non plus destinées à être une couche de sécurité vitale dans les environnements de centre de données, hybrides, multiClouds et SaaS.

Les méthodes actuelles mises en place pour tenter de résoudre ce problème engendrent de la complexité supplémentaire. Les organisations ont tendance à utiliser plusieurs outils pour gérer les identités dans toute l'entreprise, ce qui conduit à un manque de visibilité. Plus il y a d'outils dans l'environnement, plus la visibilité est mauvaise, et plus les choses sont cloisonnées et fragmentées. Il en résulte une spirale négative qui a un impact sur l'efficacité opérationnelle et crée des vulnérabilités exposant l'entreprise aux menaces.



Tous les chemins mènent à la sécurité des identités

Aujourd'hui, la question n'est pas de savoir « si » une entreprise sera victime d'une cyberattaque, mais « quand » elle la subira. Le principe de « violation présumée » ('Assume Breach') et le modèle « Zero Trust » se sont imposés comme un moyen pour les entreprises de remédier à ce problème et occupent désormais une place centrale dans leurs stratégies de sécurité. La sécurité des identités est essentielle et doit répondre aux exigences d'une mise en œuvre réussie du Zero Trust en matière de gestion des risques liés aux identités.

Adopter le principe de « violation présumée » et le modèle Zero Trust

Étant donné que les barrières traditionnelles de sécurité réseau ont été supprimées, il est très probable que votre entreprise ait déjà subi une violation. Si c'est le cas, la question est de savoir si vous êtes bien protégé. En supposant que toute identité humaine ou machine au sein de votre organisation a pu être compromise, vous devez vous concentrer sur l'identification, l'isolation et la neutralisation des menaces.

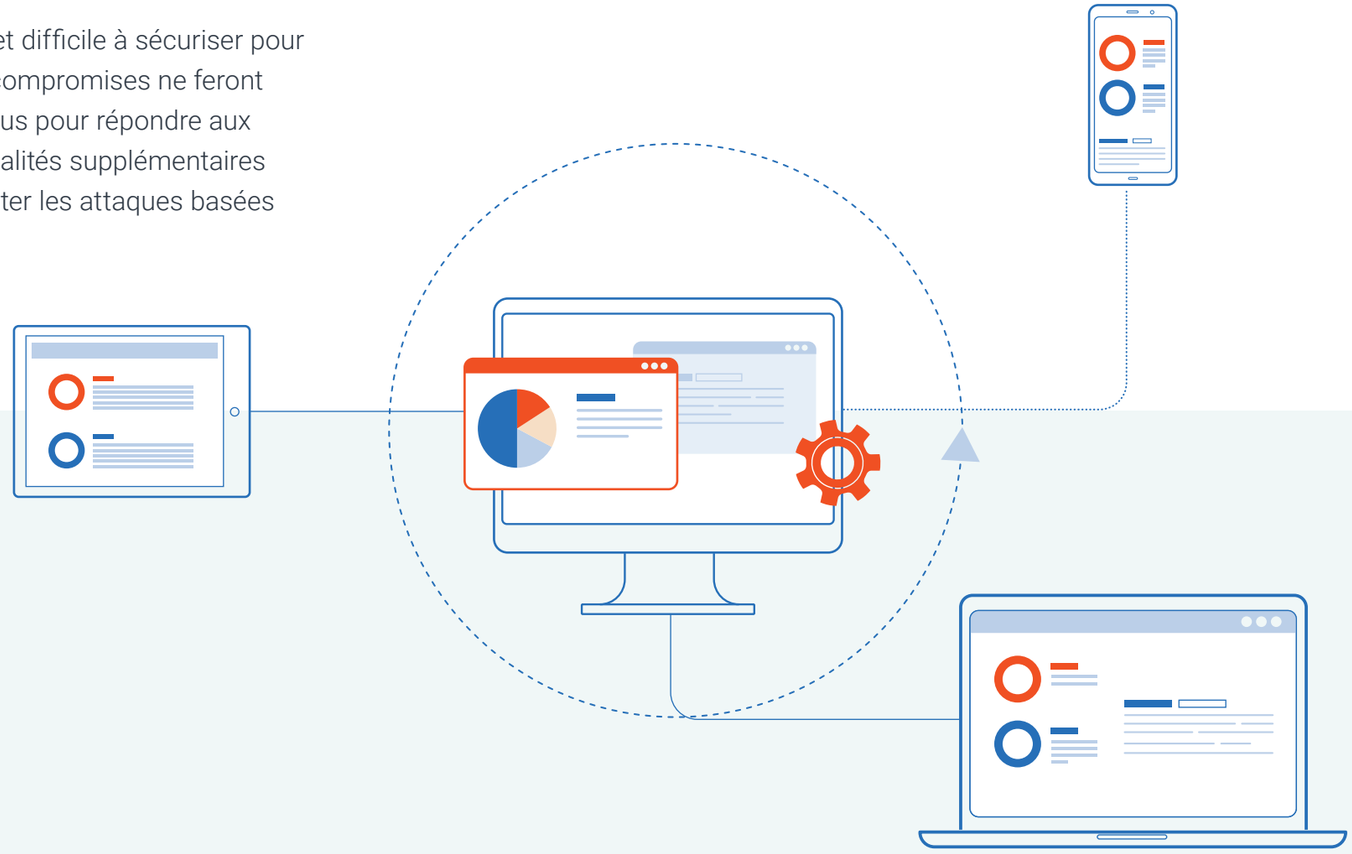
L'un des principes fondamentaux de l'architecture Zero Trust est d'authentifier et d'autoriser continuellement toutes les identités tout en accordant de manière sécurisée un accès « juste à temps » avec le bon ensemble d'autorisations.

Le problème tient en grande partie au fait que les attaques basées sur les identités sont difficiles à détecter. De nombreuses entreprises ne disposent pas de moyen fiable pour surveiller le comportement suspect des utilisateurs afin de détecter les signes indiquant que des identités ont été compromises. Cette lacune était plus facile à gérer lorsque le réseau disposait encore d'un périmètre bien défini. Aujourd'hui, dans la mesure où n'importe quelle identité, qu'il s'agisse d'un administrateur informatique, d'un fournisseur tiers, d'un utilisateur régulier, d'un compte client ou d'une machine, peut devenir un vecteur d'attaque pour les cybercriminels, ce manque de visibilité est inacceptable.

Introduction à la sécurité des identités

Alors que le paysage de l'entreprise devient de plus en plus complexe, disparate, et difficile à sécuriser pour les équipes informatiques, les risques associés aux identités susceptibles d'être compromises ne feront qu'augmenter. Dans ce contexte, les modèles IAM traditionnels ne conviennent plus pour répondre aux exigences de sécurité des identités. Les entreprises doivent ajouter des fonctionnalités supplémentaires pour sécuriser les identifiants, identifier de manière proactive les menaces et arrêter les attaques basées sur les identités lorsqu'elles se produisent.

Cette démarche nécessite de redéfinir la sécurité des identités.



Qu'est-ce que la sécurité des identités ?

Centrée sur les contrôles intelligents des privilèges, la sécurité des identités sécurise de manière transparente l'accès pour toutes les identités et automatise de manière flexible le cycle de vie de l'identité. Elle est associée à une détection et une prévention continues des menaces, créant ainsi une approche unifiée.

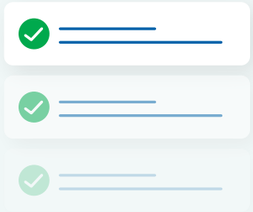
Les quatre piliers de la sécurité des identités

72 % des cadres d'entreprise s'accordent à dire que les décisions en matière de cybersécurité prises au cours des 12 derniers mois ont introduit de nouvelles vulnérabilités dans l'entreprise. Le risque d'élargissement de la surface d'attaques découle des identités ayant accès aux ressources dans plusieurs environnements. Ce risque impose à toutes les entreprises d'intégrer la sécurité des identités moderne comme élément fondamental de leur stratégie afin de se protéger contre les vulnérabilités existantes et nouvelles.

Centrée sur les contrôles intelligents des privilèges, la sécurité des identités sécurise de manière transparente l'accès pour toutes les identités et automatise de manière flexible le cycle de vie de l'identité, avec une détection et une protection continues contre les menaces, le tout au moyen d'une approche unifiée. Voici les principaux piliers de la sécurité des identités :

1 Accès transparent et sécurisé pour toutes les identités

Toutes les identités bénéficient d'un accès « juste à temps », « juste comme il faut » et sécurisé aux services, applications et ressources lorsqu'elles en ont besoin, partout et sur n'importe quel appareil.



2 Contrôles intelligents des privilèges

Les solutions de Privilege Access Management (PAM) soutiennent toutes les plateformes de sécurité des identités en fournissant des contrôles intelligents pour aider à sécuriser les identifiants où qu'ils soient et à appliquer le principe du moindre privilège.

3 Automatisation et orchestration flexibles des identités

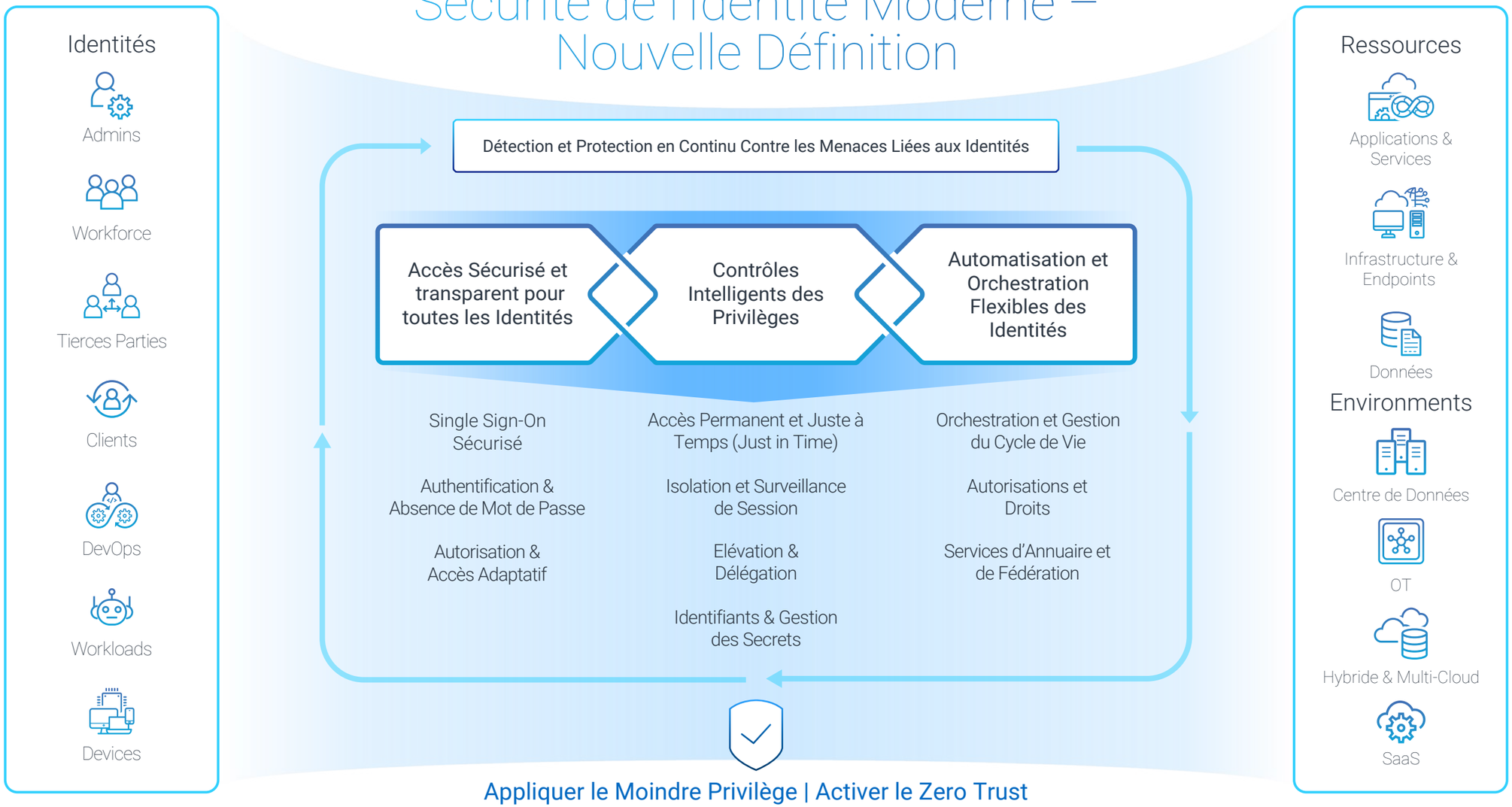
Ce pilier aide à sécuriser et à gérer de manière centralisée l'accès pour les services Web et les secrets intégrés utilisés par les applications, le pipeline DevOps et les outils d'automatisation tout au long du cycle de vie de chaque identité.

4 Détection et protection continues contre les menaces

Ce pilier permet de détecter en continu les menaces visant les identités et d'appliquer les contrôles de sécurité des identités appropriés en fonction du risque pour appliquer le principe du Zero Trust.

[4] CyberArk « 2022 Identity Security Threat Landscape Report », avril 2022

Sécurité de l'Identité Moderne – Nouvelle Définition



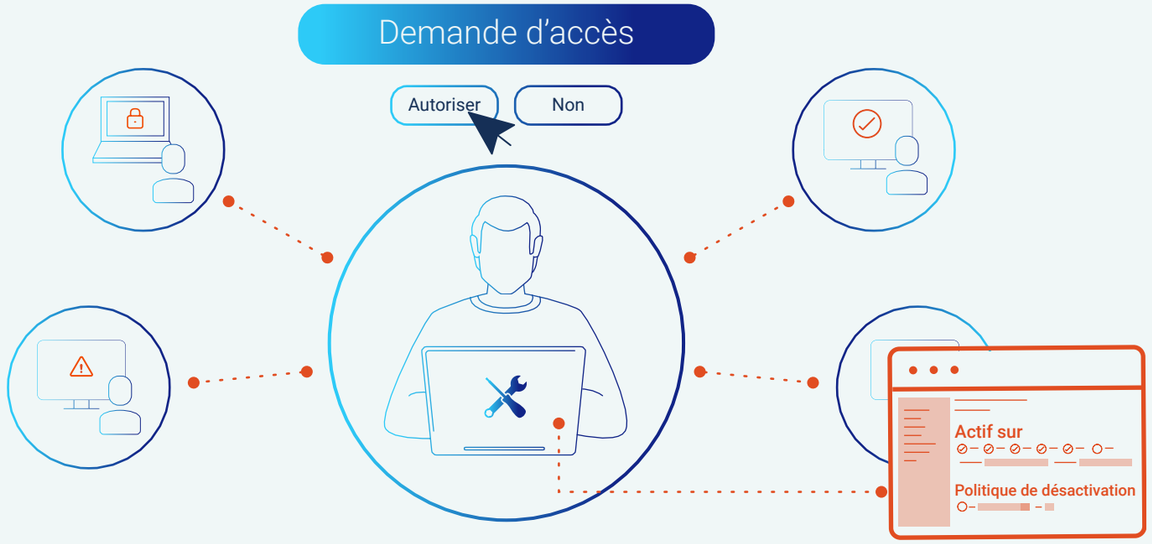
La Figure 1 montre les capacités telles que définies dans une approche moderne de la sécurité des identités.

Les contrôles des privilèges, élément fondamental de la sécurité des identités

La gestion des accès à privilèges est à la base du cadre moderne de la sécurité des identités. Elle fournit les contrôles intelligents nécessaires pour sécuriser toutes les identités où qu'elles soient, et pas seulement celles que l'entreprise surveille en tant que comptes à privilèges. Cette approche procure un dispositif de sécurité robuste pour sécuriser les identités humaines et machines dans toutes les applications, infrastructures et données avec une détection continue des menaces.

Les contrôles intelligents des privilèges tels que l'isolation et la surveillance des sessions, l'élévation et la délégation sont intégrés dans les fonctionnalités de gestion des accès et des identités, y compris la gestion du cycle de vie, les autorisations et l'authentification unique sécurisée. Cela signifie que l'accès peut être surveillé en permanence dans les centres de données, les environnements hybrides, multiClouds et SaaS, et que des contrôles intelligents de sécurité des identités peuvent être appliqués en fonction du profil de risque de chaque identité.

Par conséquent, l'accès juste à temps devient possible à tous les niveaux, et les équipes de sécurité peuvent plus facilement identifier, isoler et aider à bloquer les menaces dangereuses exploitant des identités compromises.



Exigences en matière de sécurité des identités

Il existe cinq exigences fondamentales pour adopter avec succès la nouvelle approche de la sécurité des identités :

1. **Identifier toutes les identités humaines et machines qui ont accès aux ressources.** L'entreprise doit avoir une visibilité centralisée sur l'ensemble de son parc pour détecter les identités à privilèges excessifs, les autorisations risquées et les autres menaces inconnues.

2. **Authentifier les utilisateurs grâce à un accès adaptatif en fonction du contexte.** Cette étape va au-delà d'une approche IAM traditionnelle, en aidant à arrêter les malfaiteurs s'ils parviennent à compromettre une identité.

3. **Utiliser l'autorisation dynamique, en appliquant l'accès juste à temps.** Les identités doivent recevoir le bon niveau d'autorisations nécessaires pour remplir leurs rôles, et celles-ci doivent être supprimées lorsqu'elles ne sont plus nécessaires.

4. **Sécuriser l'ensemble du processus pour améliorer la sécurité sans augmenter** les frictions qui pourraient avoir un impact sur l'expérience utilisateur et encourager les comportements à risque.

5. **Effectuer des audits unifiés** dans l'ensemble de l'environnement de l'entreprise pour s'assurer que tout est en ordre et respecter les exigences de conformité.

La valeur commerciale de la sécurité moderne des identités

Le risque de menaces internes et externes tirant parti des privilèges escaladés pour accéder à des données critiques et les extraire est une préoccupation constante pour les équipes de sécurité. Le coût moyen d'une violation de données est d'environ 4,24 millions d'euros[5], mais l'impact d'une cyberattaque réussie ne se limite pas au coût des efforts de rétablissement et aux pertes de revenus. Une attaque cause également un préjudice durable pour la marque et la réputation de l'entreprise.

L'adoption d'un cadre moderne pour la sécurité des identités permet de concilier à nouveau vitesse et sécurité. Ce cadre donne aux entreprises une approche globale, basée sur les risques, pour sécuriser toutes les identités et leur procure l'assurance que leurs actifs les plus critiques sont en sécurité.

Avantages pour l'entreprise

1. **Stimuler l'efficacité opérationnelle :** protégez l'entreprise en activant l'accès utilisateur « juste à temps » et éliminez ainsi la complexité associée à la protection des identités à grande échelle.
2. **Favoriser l'activité numérique :** accélérez les efforts de transformation numérique en proposant des expériences fiables ; trouvez le juste équilibre entre sécurité et expérience utilisateur sans friction et adoptez efficacement les services dans les environnements hybrides et multiClouds.
3. **Réduire les cyber-risques :** évitez les pertes de revenus, les temps d'indisponibilité et le vol de données critiques et de propriété intellectuelle en appliquant le principe du moindre privilège ; en cas de violation, la faille est moins susceptible de mener à un gain pour les cybercriminels, ce qui minimise l'impact des incidents de sécurité.
4. **Respecter les exigences d'audit et de conformité :** un cadre unique intègre toutes les exigences en matière d'audit et de conformité, offrant une plus grande visibilité ; cela facilite la surveillance, la gestion et l'audit de toutes les identités (administrateurs informatiques, travailleurs à distance, fournisseurs tiers, etc.) et de toutes les ressources (applications et services, données sensibles, terminaux, etc.)

[5] IBM, Rapport 2021 sur le coût d'une violation de données, juillet 2021

Plateforme de sécurité des identités de CyberArk

Alors que le paysage informatique devient de plus en plus complexe, les entreprises ont besoin de meilleurs moyens pour accorder les accès tout en sécurisant leurs activités et en se protégeant plus efficacement contre les menaces.

La plateforme de sécurité des identités de CyberArk permet de trouver ce juste équilibre. Elle permet d'adopter avec succès une approche unifiée de la sécurité des identités afin que les identités puissent accéder aux bonnes ressources au bon moment. La plateforme de sécurité des identités de CyberArk améliore l'efficacité opérationnelle en aidant l'entreprise à maintenir les malfaiteurs à l'écart tout en faisant avancer ses initiatives clés.

Principales caractéristiques :

- **Renforcement des identités du personnel :** offrez un accès simple et sécurisé aux ressources de l'entreprise grâce à l'authentification unique (SSO) et à l'authentification adaptative multi-facteurs.
- **Détection et prévention en temps réel :** la surveillance, la détection et l'atténuation des menaces continues et automatiques permettent aux entreprises de déterminer leurs points de vulnérabilité et de prendre des mesures en conséquence.
- **Visibilité de bout en bout :** un portail d'administration unique fournit une visibilité sur l'ensemble du parc de l'entreprise.
- **Accès à privilèges sécurisés :** les entreprises peuvent répertorier et gérer les identifiants et comptes à privilèges, éliminer les droits excessifs liés au Cloud, isoler et superviser les sessions à privilèges et réduire les activités risquées dans tous les environnements.
- **Sécurisation centralisée des identifiants d'application :** la gestion des identifiants permet de sécuriser tous les logiciels et outils.

Conclusion

La prolifération des identités humaines et machines a pour effet d'élargir la surface d'attaques, posant un défi pour les administrateurs de la sécurité informatique. Les cybercriminels profitent des nouveaux points d'entrée et exploitent les faiblesses des entreprises.

Afin de gérer cette multiplication des identités, il convient d'adopter une approche moderne de la sécurité des identités qui va au-delà du modèle traditionnel de gestion des identités et des accès. Cette approche doit être unifiée et fondée sur le Zero Trust et le principe du moindre privilège.

Alors que les entreprises se tournent vers l'avenir, il existe une nouvelle méthode de référence pour permettre l'innovation et la transformation de l'entreprise et réduire les risques sans restriction – et cette méthode commence par la sécurisation des identités.

CyberArk est le leader mondial de la sécurité des identités. Axée sur la gestion des accès à privilèges, la société CyberArk fournit les solutions de sécurité les plus complètes pour toutes les identités, humaines ou machines, dans les applications métiers, les effectifs distribués, les charges de travail hybrides dans le cloud et tout au long du cycle de vie du pipeline DevOps. Les plus grandes entreprises mondiales font confiance à CyberArk pour les aider à sécuriser leurs actifs les plus critiques.

États-Unis, 07/22 Doc : TSK-1822-FR (TSK-1727-EN)

CYBERARK®