La cyberrésilience à l'ère de la prolifération des identités

Comment la sécurité des identités unifiée peut remédier aux failles critiques et prendre en charge les initiatives Zero Trust

ONE IDENTITY by Quest

En tant que CISO, les préoccupations que vous avez exprimées devant le conseil d'administration à propos de la cybersécurité ont été largement éclipsées par les défis macroéconomiques, la complexité des pipelines et la nécessité de permettre une augmentation drastique des accès distants.

Nous sommes samedi matin, et votre mobile professionnel vibre dans votre bureau à domicile.

Pourquoi votre directeur de la sécurité informatique vous adresse-t-il simultanément un SMS et un appel ?

« Cela ne présage rien de bon », pensez-vous.

Et vous avez raison.

Une cyberattaque a eu lieu. Son étendue est inconnue, mais votre directeur de la sécurité informatique vous indique que son équipe évalue la situation.

Les questions se bousculent dans votre tête :

- Comment sont-ils entrés ?
- Un utilisateur interne a-t-il participé à l'attaque ?
- À quelle quantité d'informations privilégiées ont-ils eu accès ?
- Comment annoncer cela au conseil d'administration ?
- Cela va-t-il aider ou nuire au budget de cybersécurité que j'ai proposé pour le prochain exercice fiscal ?
- Dois-je mettre à jour mon CV ?

Une cyberattaque a eu lieu. Son étendue est inconnue, mais votre directeur de la sécurité informatique vous indique que son équipe évalue la situation.

Le risque de la prolifération des identités

Votre organisation a été victime de sa propre prolifération des identités. Il s'agit d'un risque de sécurité insidieux qui prend forme progressivement sous prétexte de productivité et d'innovation afin d'aider l'organisation à fonctionner plus rapidement et plus efficacement.

Cela semblait être la bonne chose à faire pour soutenir l'entreprise avec des ressources qui améliorent l'exécution de ses tâches quotidiennes. Le problème est que chaque nouveau système, application ou base de données auquel vos utilisateurs se connectent a un processus et des exigences uniques en matière de gestion des informations d'identification. Certains sont moins stricts que d'autres. Certains sont moins sécurisés que d'autres. Certains sont meilleurs. Nombre sont pires. Souvent il n'y a aucune visibilité sur les personnes qui ont accès au système et sur ce qu'elles en font.

À ces problèmes vient s'ajouter le besoin permanent de fournir un accès distant à privilèges à vos administrateurs, de gérer un nombre croissant d'utilisateurs externes se connectant à un nombre encore plus grand d'appareils, de systèmes d'exploitation et de navigateurs, et de tenter de contrôler une multitude de comptes, d'ID et de mots de passe.

Vous connaissez la prolifération des identités.

Qu'allez-vous faire pour la contrôler, la gérer et trouver un équilibre entre productivité et sécurité ?

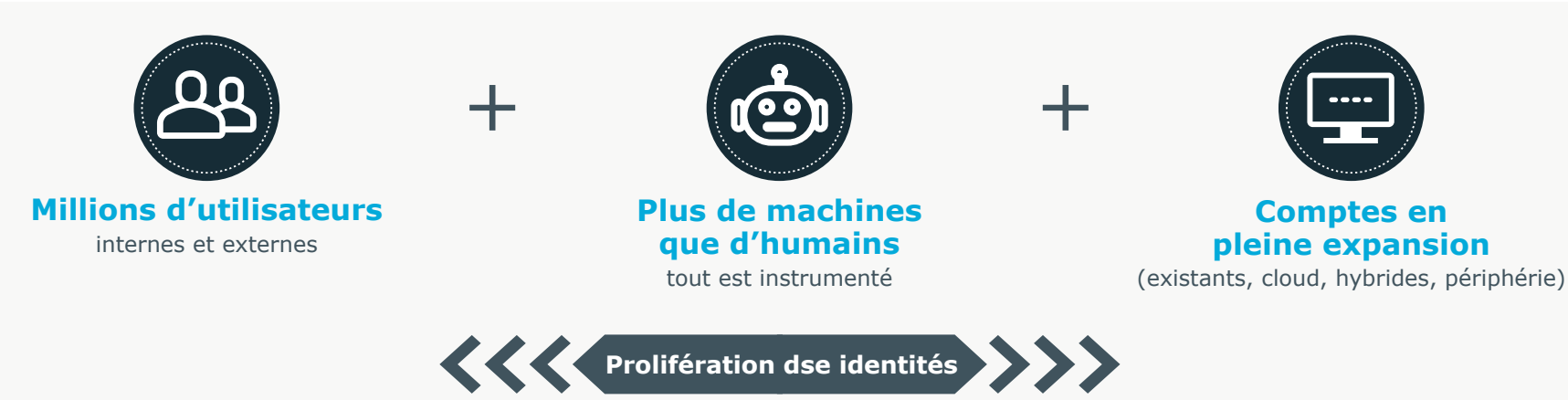
Ce qui suit est une présentation générale, en huit étapes, de la prolifération des identités. Cet e-book traite de la disparition du périmètre de sécurité traditionnel, de l'objectif de cyberrésilience et du modèle Zero Trust. Vous allez découvrir comment adopter une approche holistique et comment une plateforme de sécurité des identités unifiée peut protéger votre organisation et votre réputation.

Tendances à l'origine de la prolifération des identités

Comme décrit ci-dessus, le paysage informatique évolue sous nos yeux, ce qui a des répercussions importantes sur la façon dont les organisations doivent se protéger pour assurer la cyberrésilience. Il est difficile à suivre. Voici des exemples des changements auxquels les professionnels de la sécurité doivent rapidement s'adapter :

- La disparition rapide du bureau et de l'infrastructure traditionnels
- Les organisations dispersées doivent perdurer (les collaborateurs travaillent de plus en plus à domicile et à distance)
- Une dépendance aux sous-traitants et partenaires externes pour évoluer et développer de la valeur
- La pression pour adopter de nouvelles plateformes et technologies afin de s'adapter à l'accès distant et aux environnements de travail non traditionnels
- L'essor de l'informatique axée sur le cloud et de la distribution des services cloud sur différents sites physiques
- Le désir constant d'optimiser l'efficacité, l'accessibilité et les économies
- Complexité accrue de l'informatique due à l'adaptation aux réglementations en matière de confidentialité (RGPD, HIPAA et CCPA, par exemple) et aux processus de partage des données qui contribuent à préserver la confidentialité ou la sécurité
- L'automatisation robotisée des processus permet progressivement de simplifier des processus autrefois manuels et chronophages.

Chacune de ces tendances crée des opportunités d'efficacité et de cyberrésilience accrue, mais peut également générer de nouvelles difficultés. Pourquoi ? Le dénominateur commun de ces tendances est l'explosion des identités. Autrement dit, de plus en plus de personnes (internes et externes), de robots, de machines et d'appareils ont besoin d'accéder aux actifs des entreprises. En outre, les comptes d'utilisateurs prolifèrent, car les organisations gèrent un paysage informatique multigénérationnel. Tout cela contribue à ce qui est peut-être le plus grand défi en matière de cybersécurité à ce jour : la prolifération des identités.



ONE IDENTITY by Quest

Pourquoi il est important de maîtriser la prolifération

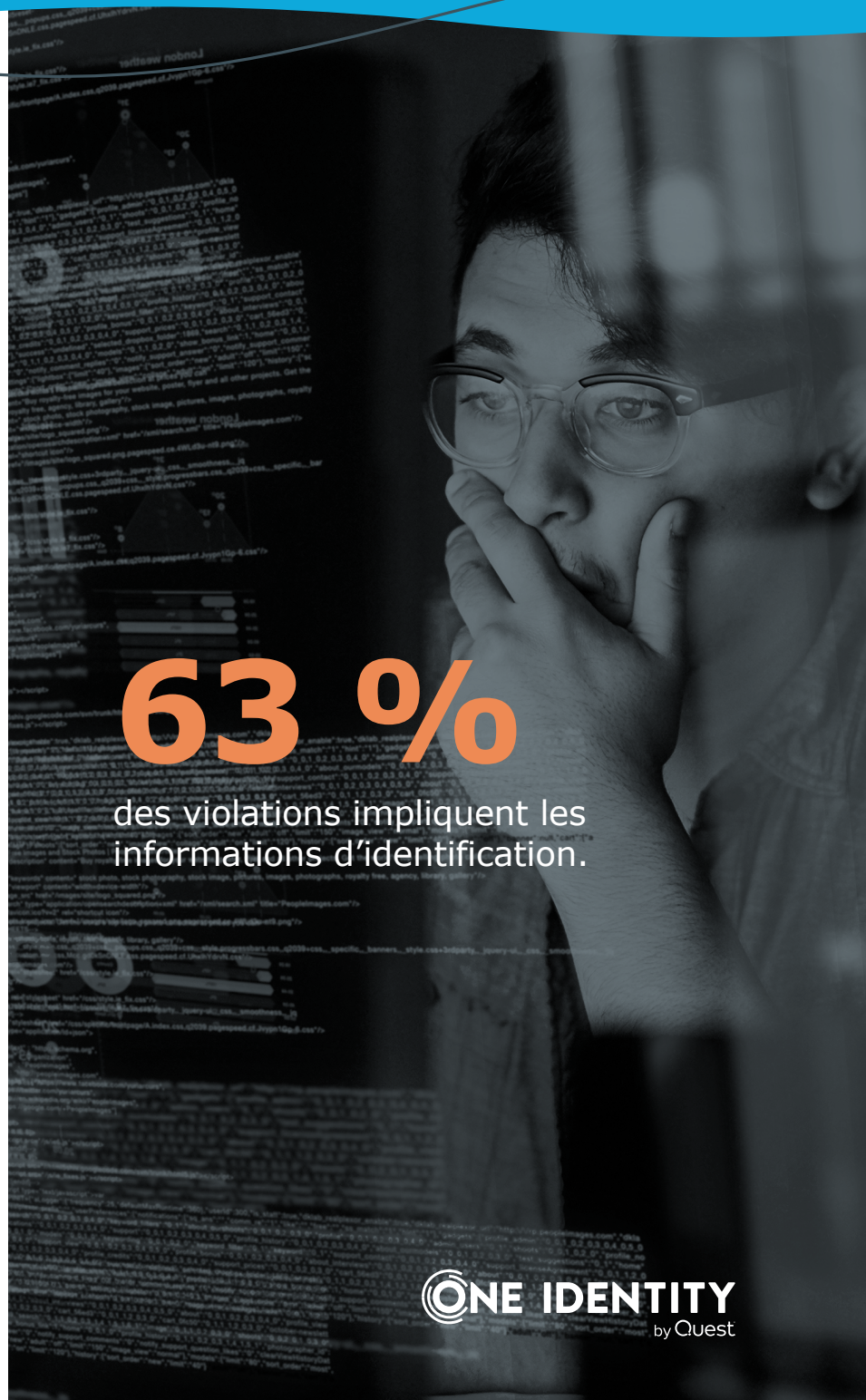
Nous savons tous que des attaquants exploitent les failles de cybersécurité partout où elles existent et souvent à grande échelle. Cela se produit en temps réel avec la prolifération des identités, car nous avons observé récemment une augmentation massive des attaques par vol d'identités et d'informations d'identification.

Ainsi, d'après le rapport d'enquête 2021 sur les compromissions de données (DBIR) de Verizon, 63 % des violations impliquaient des informations d'identification. Selon CensusWide, ce sont près de la moitié des organisations interrogées qui ont été touchées par un vol d'informations d'identification à privilèges au cours de l'année précédente.

Vous pouvez voir pratiquement tous les jours l'impact dévastateur de ces failles liées aux identités à la une des sites d'informations. Le piratage de SolarWinds, la cyberattaque de Colonial Pipeline et la vulnérabilité d'Exchange Server ne sont que quelques exemples d'incidents très visibles. Ces violations ont impacté non seulement la sûreté, les moyens de subsistance et la sécurité des citoyens lambda, mais elles ont également eu des répercussions négatives sur les organisations.

De plus, certaines attaques auraient facilement pu être déjouées. D'après un récent rapport de Cybersecurity Insiders, près de la moitié des utilisateurs disposent de plus de privilèges qu'ils n'en ont besoin pour leur travail. C'est pourquoi, vous voyez non seulement les entreprises prioriser les identités et les privilèges, mais aussi les gouvernements souligner leur importance relative. Dans une première version de note de service en septembre 2021, le Ministère du Budget américain a souligné une série de résultats à atteindre d'ici la fin de l'exercice fiscal 2024, notamment l'adoption par les agences gouvernementales de l'authentification multifacteur et la mise en place de processus de gestion des identités à l'échelle de l'entreprise.

Pour que les organisations puissent combler ces lacunes en matière de cybersécurité, elles doivent maîtriser la prolifération des identités, sous peine de se voir infliger des amendes, de connaître des poursuites judiciaires et de perdre la confiance et les revenus des clients.



L’essor de l’identité comme nouveau périmètre

Les difficultés liées aux identités étant de plus en plus fréquentes et avec de fortes répercussions, il est logique que la sécurité des identités prenne de plus en plus d’importance.

Le périmètre traditionnel reste une défense importante contre les cyberattaques, mais à bien des égards, il était fait pour une autre époque. Cette approche centrée sur l’infrastructure, qui a été la pièce maîtresse des stratégies de cybersécurité pendant de nombreuses années, repose sur l’idée qu’il est possible de tout protéger dans l’entreprise. Naturellement, la seule façon d’atteindre cet objectif ambitieux est d’optimiser votre défense au niveau des points les plus éloignés où il est possible d’empêcher une compromission.

Avec le périmètre de sécurité en passe de devenir obsolète, cette approche n’est tout simplement pas pratique et est dépassée. Les responsables de la sécurité informatique reconnaissent désormais que les compromissions sont inévitables. De ce fait, une stratégie plus pragmatique consiste à prendre des mesures pour empêcher les attaquants d’entrer, mais aussi pour empêcher l’exploitation des failles une fois qu’ils sont sur le réseau. Avec cette approche centrée sur les identités, les organisations tournées vers l’avenir donnent la priorité à ce qui est essentiel, puis prennent des mesures pour tout vérifier avant d’accorder l’accès en premier lieu. Elles vérifient par exemple l’identité d’un utilisateur, à quoi il doit avoir accès, ce qu’il fait avec une autorisation donnée et quand ses droits doivent changer.

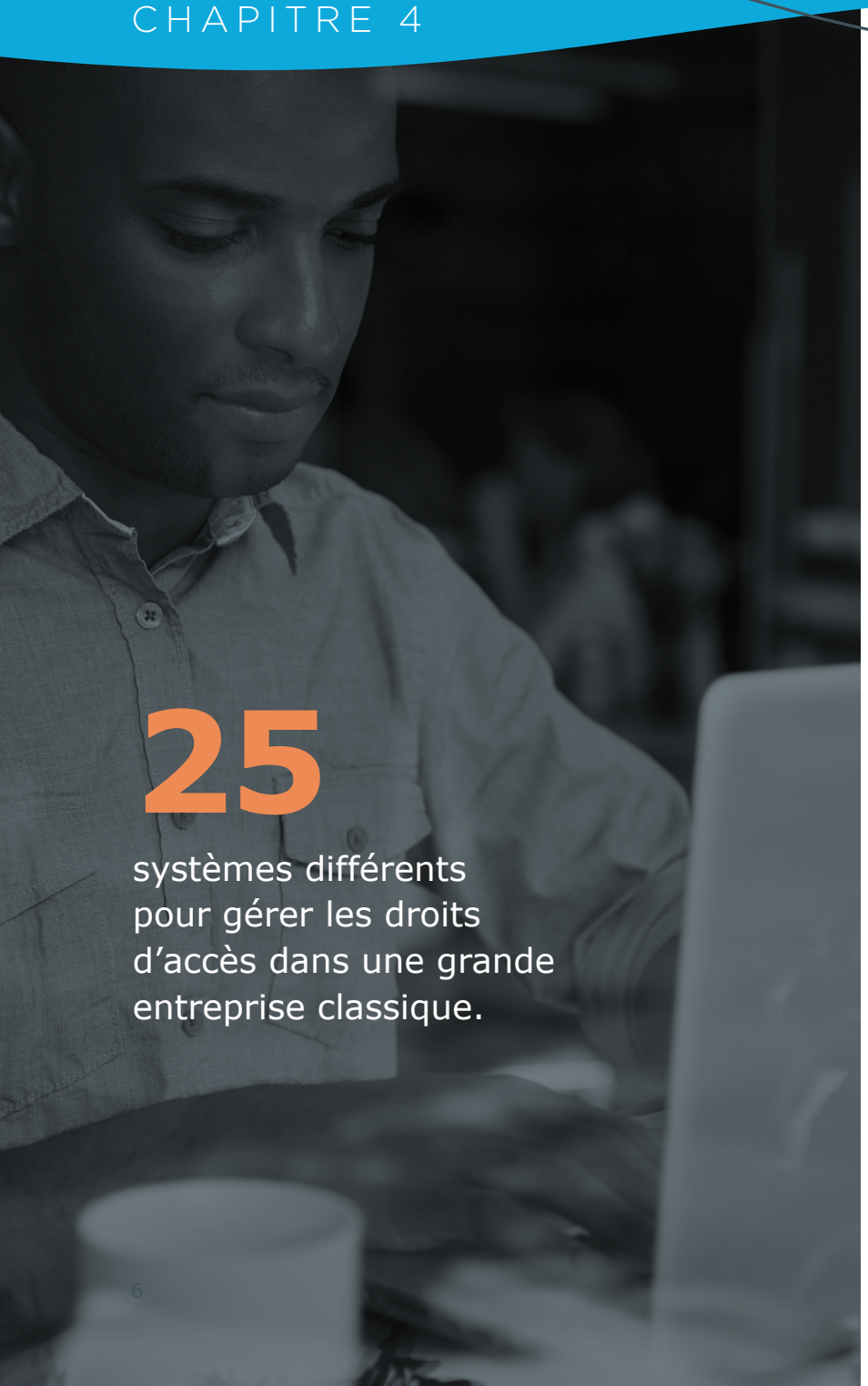
En bref, l’efficacité du périmètre traditionnel étant amoindrie, c’est l’identité qui émerge comme nouvel atout.

Approche **centrée sur l’infrastructure**

Tout PROTÉGER

Approche **centrée sur les identités**

Tout VÉRIFIER



25

systèmes différents pour gérer les droits d'accès dans une grande entreprise classique.

Principaux obstacles à la cyberrésilience

Si la sécurité des identités est une tendance émergente clé, la réussite de sa mise en place n'est pas toujours simple. Cela est dû en grande partie à la façon dont les identités évoluent. Auparavant, les organisations étaient principalement préoccupées par les collaborateurs internes qui étaient embauchés pour un seul travail, qui étaient liés au bureau et qui accédaient aux ressources à partir d'un seul point. La plupart des identités étaient des utilisateurs.

Si l'on compare cette situation à celle d'aujourd'hui, on constate que la dynamique est totalement différente. Non seulement les professionnels de la sécurité doivent se préoccuper des collaborateurs internes, mais ils doivent également prendre en compte les identités des sous-traitants, des fournisseurs et des partenaires. Au lieu d'effectuer un seul travail, les collaborateurs ont tendance à changer fréquemment de fonction ; ils ne sont pas liés au bureau et accèdent à ce dont ils ont besoin à partir de plusieurs points. De plus, les professionnels de la sécurité doivent non seulement prendre en compte les utilisateurs, mais également les applications et les machines. Les utilisateurs peuvent désormais avoir plusieurs identités dans un nombre encore plus grand de comptes ; ils peuvent être des machines et des robots, et les utilisateurs humains peuvent posséder plusieurs appareils se connectant à différentes versions ou générations d'applications. Ils peuvent également se déplacer pour atteindre des ressources à partir de différents systèmes et points d'accès physiques.

En outre, la plupart des organisations gèrent aujourd'hui les droits d'accès en silos. Selon le rapport « Third Annual Global Password Security Report », les grandes entreprises moyennes gèrent des identités dans 25 systèmes différents. Cet environnement large et varié peut empêcher l'équipe de sécurité informatique d'obtenir une visibilité complète sur les activités des utilisateurs. Il empêche également l'équipe d'appliquer des analyses complètes. Ces difficultés sont à l'origine de lacunes et d'incohérences et peuvent constituer un obstacle à la vérification complète avant d'accorder l'accès aux utilisateurs, ce qui est un élément essentiel de la mise en œuvre d'une approche moderne de la sécurité.

Si votre organisation ne parvient pas à combler ces lacunes, elle risque de ne pas pouvoir s'adapter à l'évolution des rôles/responsabilités des utilisateurs, aux changements de l'infrastructure informatique et à l'apparition de nouvelles menaces. Combler correctement ces lacunes contribuera à la cyberrésilience de votre organisation.

Le cas d'une approche holistique pour la sécurité des identités

La sécurité des identités est flexible et peut prendre des formes très différentes en fonction des utilisateurs et de leurs besoins, et des ressources auxquelles ils sont connectés et qui constituent une entreprise. La clé du succès est de passer d'une sécurité des identités fragmentée à un état unifié.

De nombreuses organisations abordent séparément les formes principales de la sécurité des identités : gouvernance et administration des identités, gestion des accès et des identités, gestion des comptes à privilèges et gestion et sécurité d'Active Directory. Pour chacune de ces formes, il y a souvent plusieurs silos à prendre en compte, et les utilisateurs, les applications et les données sont tous gérés distinctement. Cet état de fragmentation crée de nombreuses frictions, empêche l'automatisation et oblige les organisations à se demander quand et comment gérer les droits d'accès.

Le modèle émergent est bien plus holistique, les principales formes de sécurité des identités étant traitées ensemble. Ainsi, les applications se chevauchent, les silos de données s'amenuisent, et les personnes, les applications et les données sont alignées comme un tout. Avec cette approche de sécurité des identités unifiée, vous pouvez corréler toutes les identités, supprimer les frictions grâce à une meilleure intégration, réduire votre surface d'attaque et renforcer votre cyberrésilience.

ONE IDENTITY by Quest

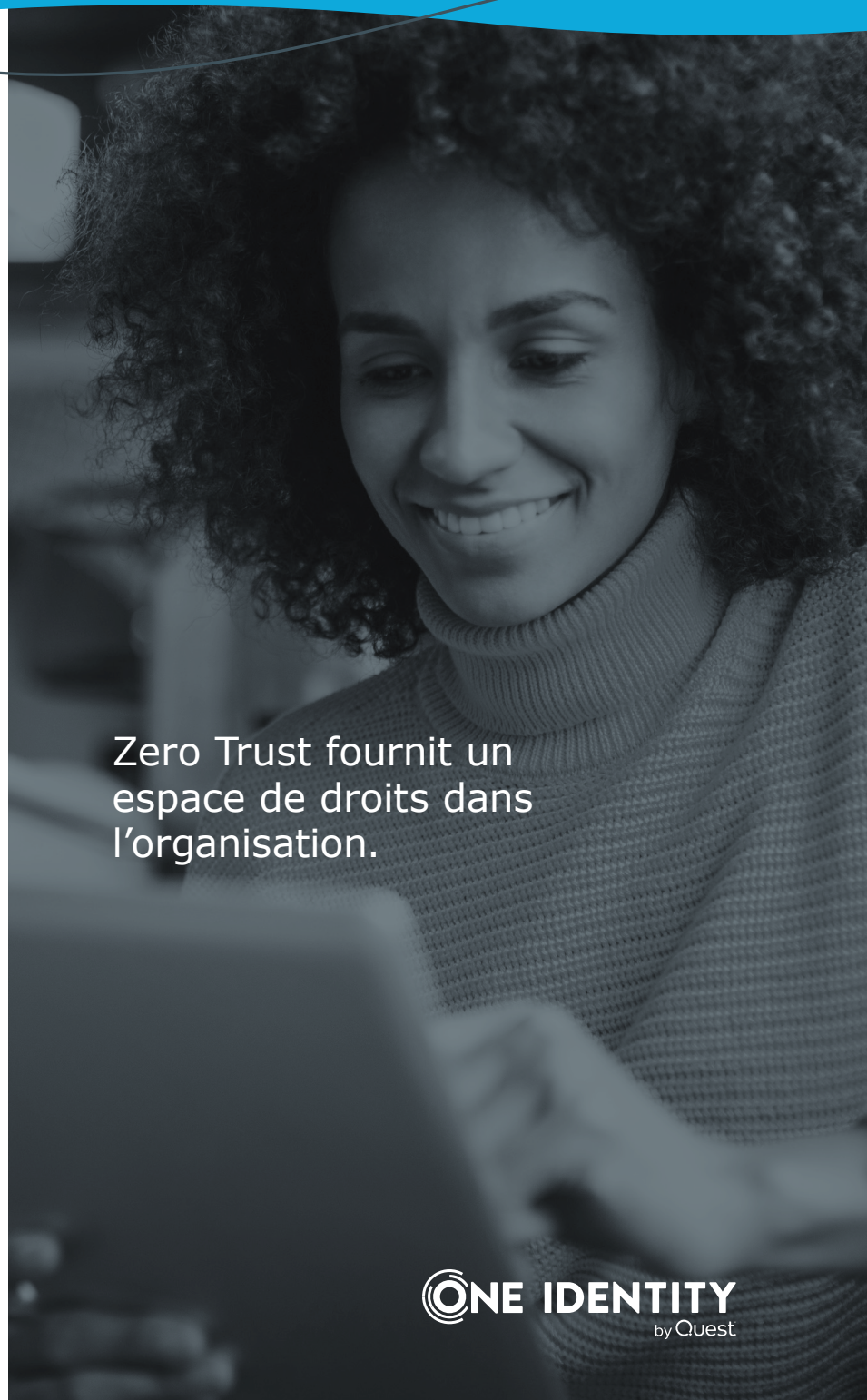
La sécurité des identités unifiée comme principal module de Zero Trust

Il est désormais largement admis que Zero Trust est un modèle éprouvé pour la mise en œuvre d'une sécurité solide et sélective. Il élimine les autorisations vulnérables, les accès inutiles et excessifs au profit d'une délégation de droits spécifiques et d'un provisioning avec granularité. Passer d'un état fragmenté à un état unifié en matière de sécurité des identités permet aux organisations de faire un pas de géant pour tenir cette promesse.

Le succès de Zero Trust commence par la mise en place d'un dispositif suffisamment large. Il faut ainsi se concentrer non seulement sur les identités des personnes, mais aussi sur celles des machines, ainsi que sur les comptes en pleine expansion à mesure que les organisations évoluent vers un paysage informatique multigénérationnel, hybride et en périphérie. Si vous tracez un cercle trop petit, vous risquez de laisser la porte ouverte aux attaquants. L'unification de votre stratégie de sécurité des identités vous permet d'éviter ce problème.

Un deuxième élément clé de Zero Trust est de fournir un espace de droits d'accès dans l'organisation. Grâce à la visibilité et aux informations supplémentaires dont ils disposent, les professionnels de la sécurité peuvent plus rapidement et plus efficacement ajouter, supprimer et ajuster les privilèges juste-à-temps. Ce faisant, ils peuvent contrôler l'accès des utilisateurs à ce qui est nécessaire pour effectuer leur travail uniquement, et seulement au bon moment, tout en éliminant les processus manuels sujets aux erreurs et la lourde implication de l'équipe informatique.

Enfin, un élément clé de Zero Trust est l'adaptabilité, qui est rendue possible par une stratégie de sécurité des identités unifiée. En utilisant une approche holistique qui inclut la connaissance du contexte et l'analyse du comportement, les organisations peuvent plus rapidement et plus efficacement anticiper, détecter et prendre des mesures correctives pour faire face aux menaces émergentes.



Bonnes pratiques pour unifier votre approche en matière de sécurité des identités

La technologie peut améliorer considérablement les chances de succès d'une organisation en unifiant la sécurité des identités, mais que doivent rechercher les professionnels de la sécurité chez un fournisseur de solutions afin d'optimiser leurs résultats ? Vous trouverez ci-dessous cinq points essentiels à prendre en compte lorsque vous envisagez des alternatives :

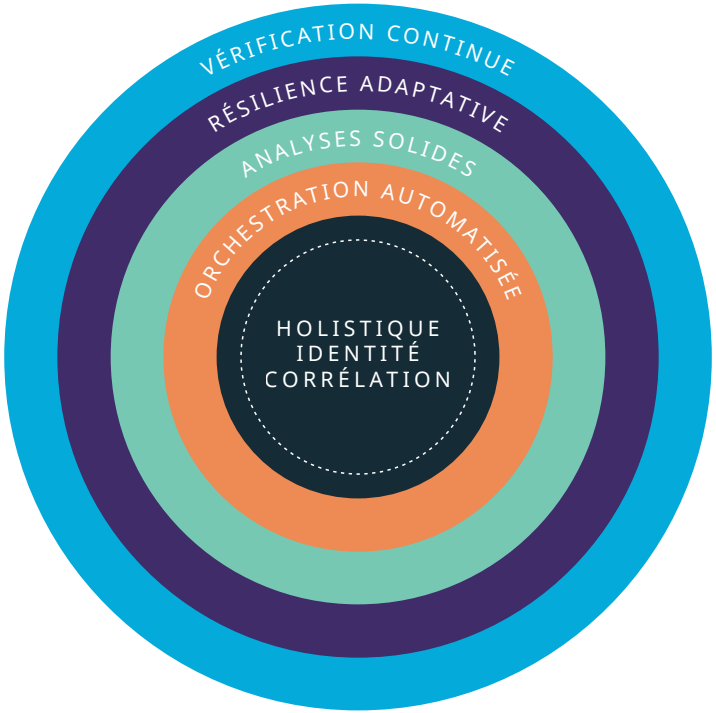
1. **Corrélation holistique :** avant tout, les organisations ont besoin d'unifier de bout en bout l'ensemble des identités et des comptes afin d'optimiser leur visibilité et de prendre des décisions en toute connaissance de cause.

2. **Orchestration automatisée :** le deuxième élément principal d'une stratégie de sécurité des identités unifiée est une gouvernance sans frictions, dans la gestion des identités et des privilèges. Vous pouvez ainsi optimiser l'efficacité à grande échelle.

3. **Analyses solides :** compte tenu de l'ampleur et de la nature évolutive de la sécurité des identités, les organisations ont besoin de solutions qui fournissent les informations nécessaires pour anticiper, détecter et prendre des mesures correctives sur les menaces émergentes à grande échelle.

4. **Cyberrésilience adaptative :** en reconnaissant que les menaces et l'entreprise ne sont plus statiques, les professionnels de la cybersécurité doivent pouvoir changer rapidement en fonction des besoins et préparer leurs investissements pour l'avenir.

5. **Vérification continue :** la sécurité des identités unifiée est plus efficace lorsque vous pouvez tout vérifier avant l'octroi des accès. La technologie enrichie avec la connaissance de la situation, la surveillance des sessions et l'analyse des comportements contribuera au succès.



Problèmes clés résolus avec la sécurité des identités unifiée

Jusqu'à présent, nous avons présenté les difficultés et avantages généraux d'une approche unifiée de sécurité des identités. Mais quels sont les cas d'utilisation spécifiques auxquels les responsables de la cybersécurité peuvent s'attendre avec une telle stratégie ? Voici quelques résultats courants :

Problèmes clés	Cas d'utilisation	Résultats
Sécuriser l'organisation : **Protéger vos collaborateurs, applications et données**	• Zero Trust : protéger à grande échelle et réduire le risque de violations en créant un cadre Zero Trust • Accès distant à privilèges : s'assurer que les télétravailleurs et les sous-traitants peuvent accéder aux informations essentielles en toute sécurité, sans frictions de VPN • Gestion des privilèges des terminaux : unifier la sécurité des terminaux pour les postes de travail AD/ Azure AD, Unix/Linux, Windows et macOS • Analyses des comptes à privilèges et arrêt des sessions : détecter les risques parmi vos utilisateurs à privilèges et éviter les préjudices pour votre organisation • Gestion et sécurité de l'environnement AD hybride : réduire l'implication de l'équipe informatique dans les tâches de provisioning et éliminer les erreurs manuelles • Sécurité à privilèges de l'environnement AD/Azure AD : sécuriser votre environnement interne aussi étroitement que le périmètre pour protéger vos actifs essentiels et souvent ciblés • Coffre-fort de mots de passe : simplifier la gestion des mots de passe et protéger vos informations d'identification à privilèges	• Élimination des vulnérabilités et du risque • Implémentation de Zero Trust • Prévention des violations • Unification des identités dans les environnements cloud et sur site • Accès à privilèges sécurisé
Optimiser l'efficacité opérationnelle : **centraliser les processus de sécurité**	• Gouvernance des accès à privilèges : réduire les fossés en matière de stratégie et de sécurité entre les identités disposant d'un accès à privilèges et celles des utilisateurs standard • Gestion et sécurité d'Active Directory : sécuriser et gérer les utilisateurs et les groupes, et contrôler l'accès des administrateurs via la délégation • Pont Active Directory : unifier la gestion basée sur des stratégies dans l'ensemble de vos systèmes d'exploitation et plateformes • Fusions et acquisitions : s'adapter sans heurts aux modifications, par exemple aux actions de la main-d'œuvre et aux pandémies, qui nécessitent généralement une intervention manuelle importante	• Unification des stratégies et processus de gestion des identités • Amélioration considérable de l'efficacité • Contrôle de l'accès aux ressources, systèmes et plateformes • Automatisation des tâches courantes pour optimiser le travail de l'équipe informatique • Utiliser facilement les processus des JML (Joiners, Movers, Leavers : nouvelles recrues, changements de poste, départs)

Problèmes clés	Cas d'utilisation	Résultats
Respecter les exigences de conformité et d'audit : **Gérer la prolifération des identités et prouver le respect de la stratégie**	• Gouvernance des identités : s'assurer que les stratégies sont appliquées, que l'accès des utilisateurs est géré conformément aux exigences et être en mesure d'en apporter la preuve • Audit des sessions sans agent : protéger vos ressources stratégiques et vos utilisateurs à l'aide de l'automatisation des enregistrements et des analyses. Prendre également en charge des analyses forensiques et satisfaire aux exigences de conformité de l'accès à privilèges. • Création de rapports de conformité immédiats : bénéficier des fonctionnalités de création de rapports en temps réel sur les mesures de conformité des utilisateurs et des ressources de votre entreprise afin de satisfaire aux exigences des auditeurs et de la conformité	• Respect des exigences des auditeurs concernant les informations liées aux autorisations • Réduction et élimination des risques de violation des stratégies centrées sur l'identité • Création de pistes d'audit fiables pour l'ensemble de l'activité des sessions à privilèges • Mise en place d'équipes de sécurité pour rechercher des événements spécifiques et visionner de nouveau les sessions à privilèges • Respect des besoins de conformité pour surveiller les accès à privilèges
Sécuriser votre transformation numérique : **protéger les identités tout en augmentant les fonctionnalités et les accès**	• Orchestration de la sécurité DevOps : sécuriser les pipelines DevOps avec une sécurité centrée sur les identités • Gouvernance des applications : simplifier les décisions d'accès aux applications et permettre aux responsables des opérations de prendre des décisions éclairées • Optimisation de la sécurité de la RPA : gérer les risques associés à la prolifération des identités de la RPA • Gestion des environnements complexes : réduire les coûts d'administration des environnements hétérogènes pour optimiser la sécurité, la vitesse et la prise de décisions	• Gestion fluide de votre environnement hybride • Adoption de pratiques RPA en toute sécurité • Facilité d'utilisation des secrets DevOps • Augmentation des responsabilités des collaborateurs et sous-traitants • Réduction du nombre d'erreurs, renforcement de la sécurité, optimisation de l'efficacité et simplification des processus

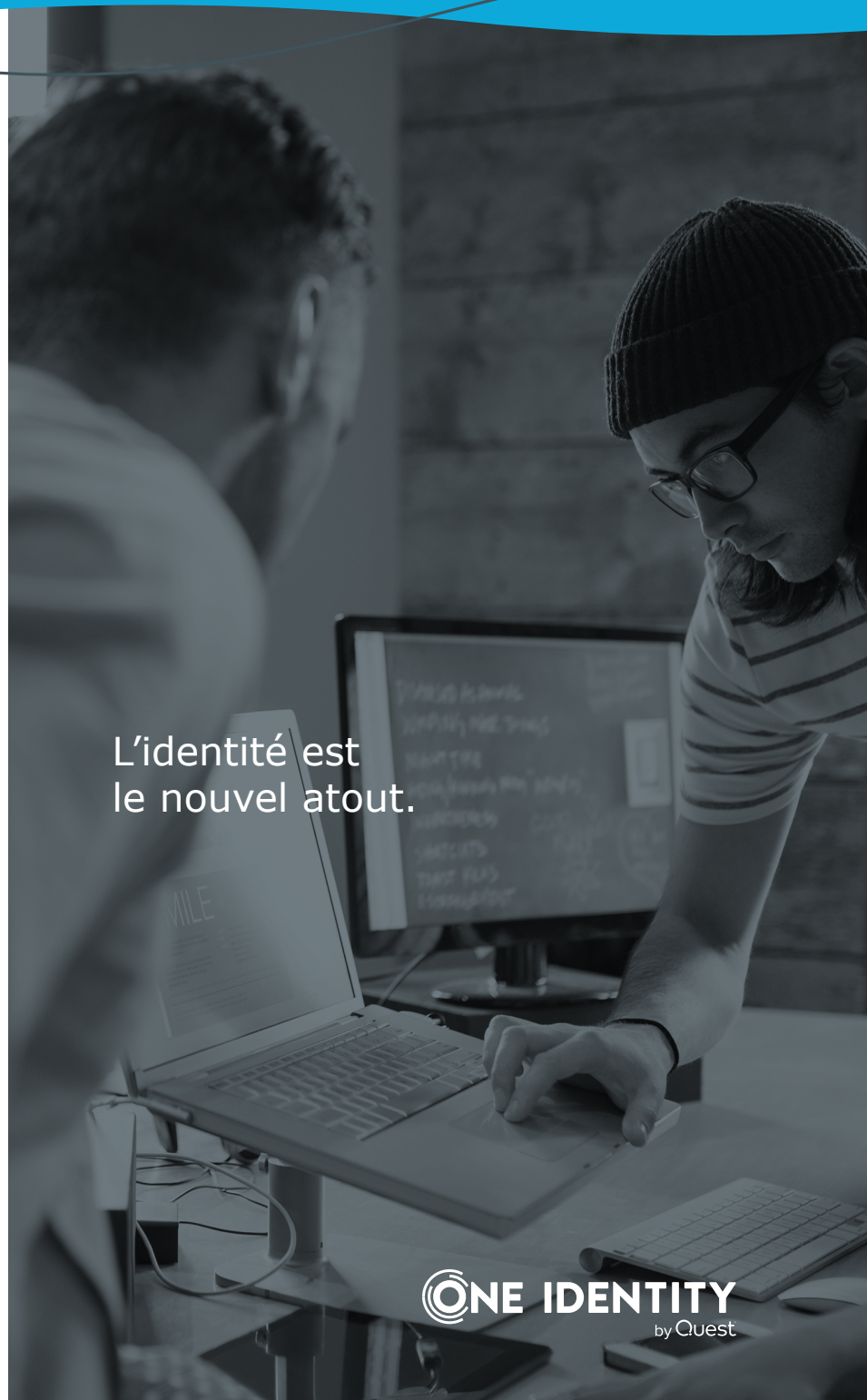
Conclusion

Des forces puissantes sont à l'œuvre, et l'évolution rapide des entreprises et du paysage informatique contribue à la prolifération des identités. Cette prolifération s'amplifie chaque jour. Elle crée des risques bien réels que les professionnels de la cybersécurité doivent prendre au sérieux. Il est temps de cesser de gérer la cybersécurité de manière fragmentée.

En adoptant une approche holistique pour gérer les droits d'accès, les CISO peuvent combler les failles de cybersécurité critiques, renforcer la cyberrésilience de leur organisation et franchir un pas important pour tenir la promesse de Zero Trust qui devient rapidement un impératif d'entreprise.

L'identité est le nouvel atout. Une stratégie de sécurité des identités unifiée permet de lutter contre les méthodes d'attaque modernes et de faire entrer votre organisation dans le futur.

Désormais, lorsque votre directeur de la sécurité informatique vous appellera, vous saurez que vous disposez des informations nécessaires pour évaluer immédiatement l'état de la sécurité de vos identités et recenser les mesures qui ont été prises sur votre réseau.



À propos de One Identity

One Identity propose des solutions de sécurité des identités unifiée qui aident les clients à augmenter leur niveau global de cybersécurité et protéger les collaborateurs, applications et données essentiels à leur activité. Notre plateforme de sécurité des identités unifiée regroupe les meilleures fonctionnalités (administration et gouvernance des identités, gestion des accès et des identités, gestion des comptes à privilèges et gestion et sécurité d'Active Directory) pour permettre aux organisations de passer d'une approche fragmentée à une approche holistique en matière de sécurité des identités. La solution One Identity est fiable et reconnue à l'échelle de la planète : elle gère plus de 250 millions d'identités pour plus de 5 000 organisations dans le monde. Pour plus d'informations, rendez-vous sur www.oneidentity.com.

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :
www.quest.com/fr-fr/company/contact-us.aspx.

eBook-UnifiedIdentitySecurity-KA-FR-WL-69156

ONE IDENTITY by Quest