SailPoint

Livre interactif

2024-2025

Les Horizons de la Sécurité des Identités

Exploiter la puissance de la sécurité des identités numériques pour infléchir la courbe de valeur de la cybersécurité

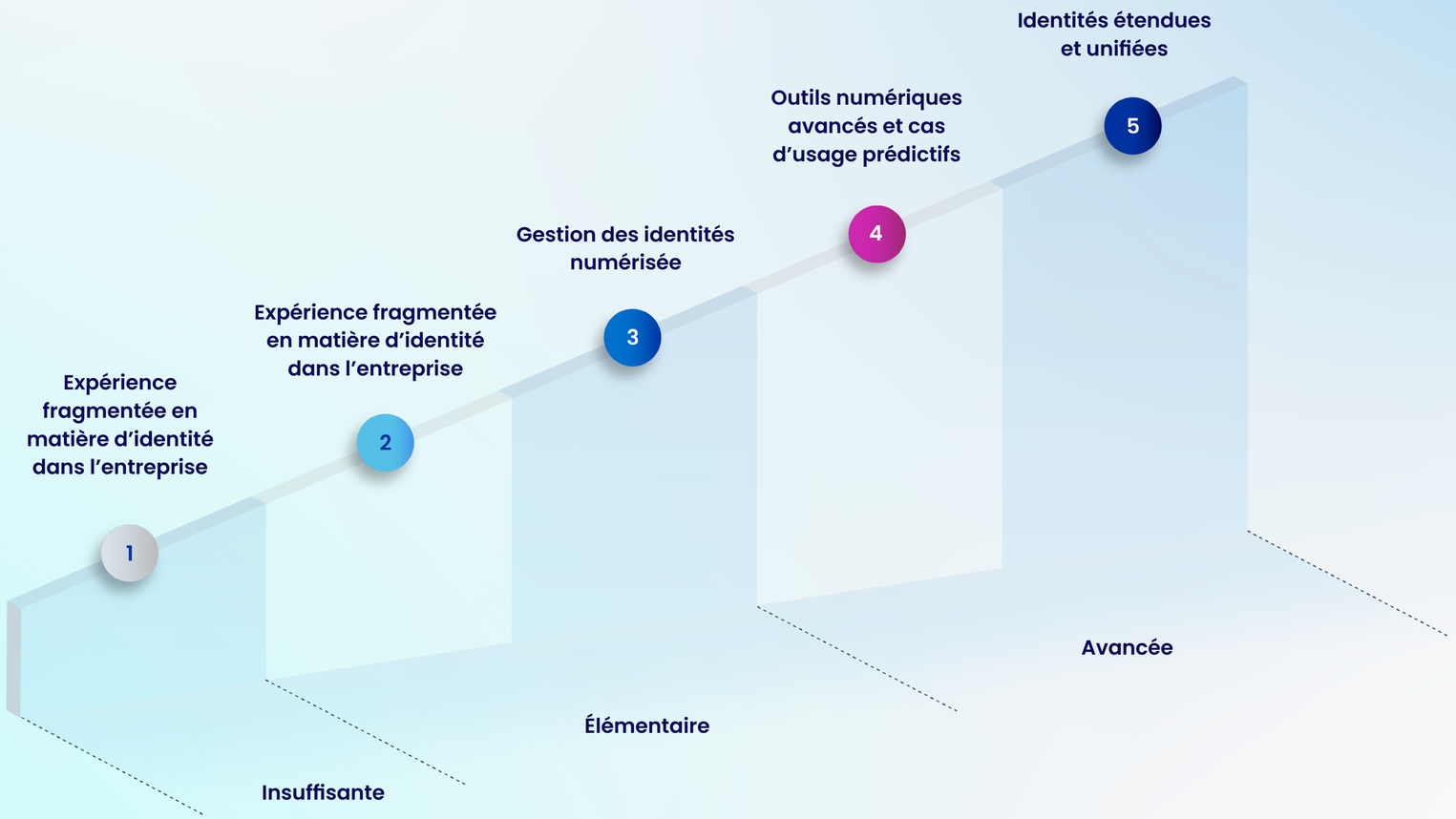
Commencer →

La voie vers une sécurité des identités plus mature

Les entreprises du monde entier, tous secteurs confondus, font face à un double défi : contrer des cybermenaces toujours plus sophistiquées et omniprésentes, tout en composant avec des contraintes budgétaires et des réductions de coûts récurrentes.

Le domaine de la sécurité des identités subit une pression particulièrement forte : les surfaces d'attaque augmentent et les budgets informatiques s'amenuisent à mesure que les entreprises prennent de l'ampleur, alors même que les parties prenantes, qu'elles soient internes ou externes, exigent une amélioration permanente de la sécurité et de l'expérience numérique des utilisateurs.

Au cours des trois dernières années, SailPoint a interrogé des responsables de la gestion des identités et des accès (IAM) dans le monde entier afin d'évaluer leurs capacités à travers cinq horizons de la sécurité des identités. Parmi les 350 décideurs interrogés en juillet 2024 se trouvent des cadres supérieurs en charge des technologies de l'information, de la cybersécurité et de la gestion du risque. Plus de la moitié d'entre eux travaillent pour des entreprises comptant plus de 10 000 salariés, dans les secteurs de la finance ou de la haute technologie.



Source : tous les graphiques de ce document sont tirés du rapport 2024-2025 : **Les Horizons de la Sécurité de Identités.**

CHAPITRE 1

Les progrès technologiques façonneront l'avenir de la sécurité des identités numériques

Commencer le chapitre →

L’avenir de l’identité sera régi par 4 éléments clés

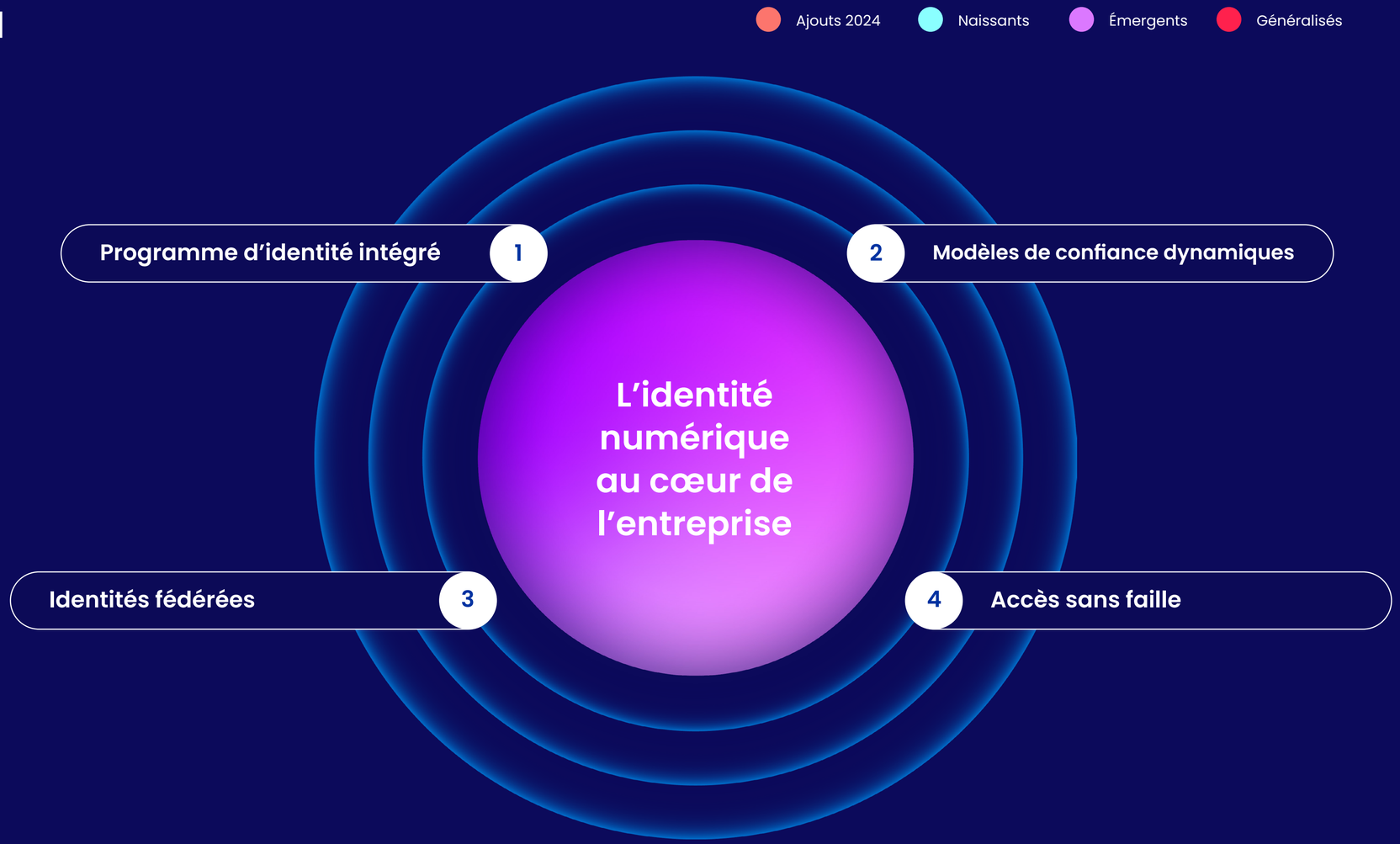
Ces dernières années, nos observations et nos recherches ont confirmé que l’avenir de la sécurité des identités sera façonné par des programmes intégrés de sécurité des identités.

Les principaux éléments sont présentés ici, accompagnés des tendances qui les complètent.

En constante évolution, la réglementation et les risques continuent de façonner ces quatre éléments.

La structure de sécurité des identités deviendra le centre névralgige des futures opérations de sécurité.

La prolifération des réglementations et de normes sectorielles liées à la sécurité des identités, dans le monde entier et dans les différents secteurs d’activité, suscitera des attentes plus fortes en la matière.



L’avenir de l’identité sera régi par 4 éléments clés

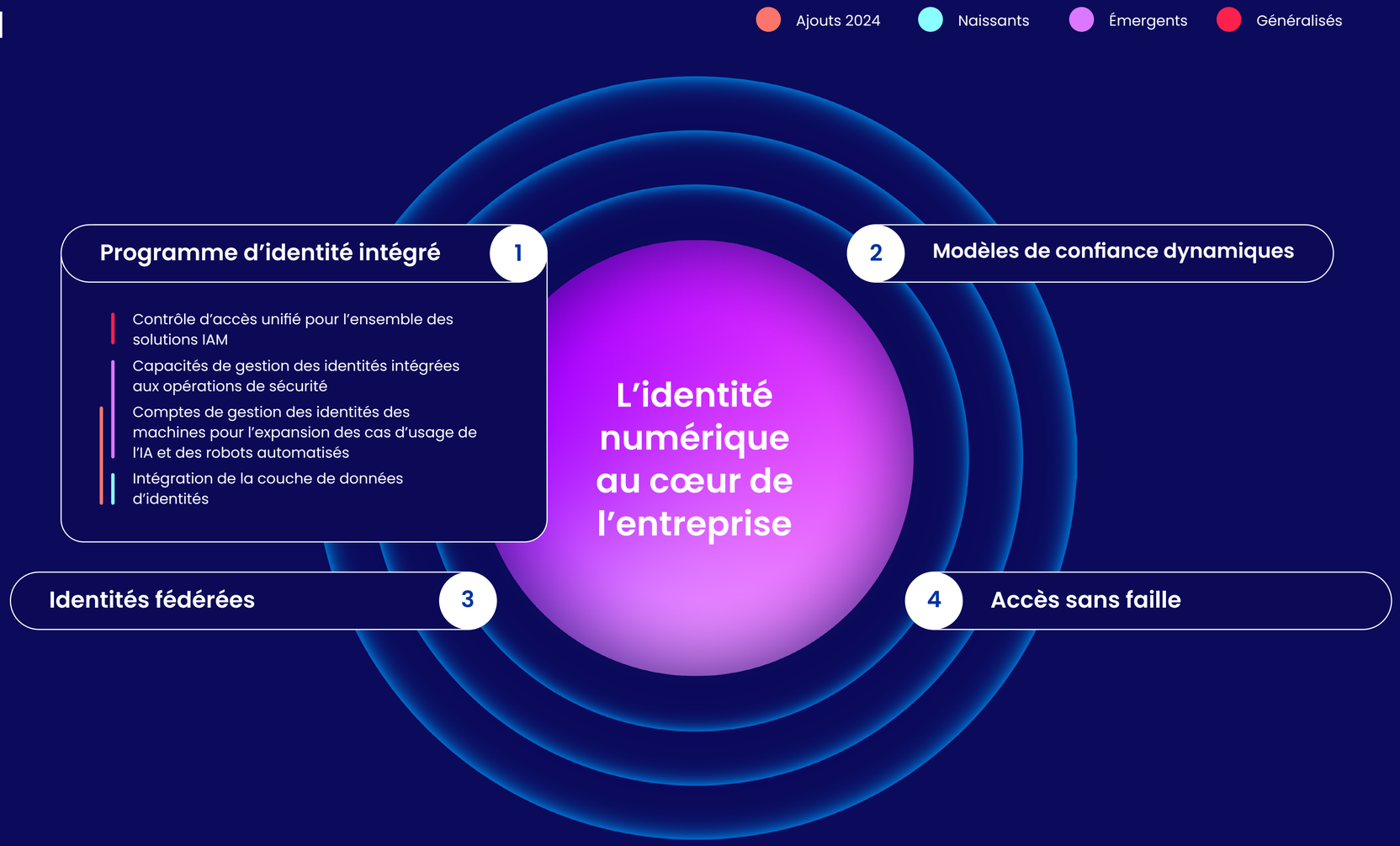
Ces dernières années, nos observations et nos recherches ont confirmé que l’avenir de la sécurité des identités sera façonné par des programmes intégrés de sécurité des identités.

Les principaux éléments sont présentés ici, accompagnés des tendances qui les complètent.

En constante évolution, la réglementation et les risques continuent de façonner ces quatre éléments.

La structure de sécurité des identités deviendra le centre névralgige des futures opérations de sécurité.

La prolifération des réglementations et de normes sectorielles liées à la sécurité des identités, dans le monde entier et dans les différents secteurs d’activité, suscitera des attentes plus fortes en la matière.



L'avenir de l'identité sera régi par 4 éléments clés

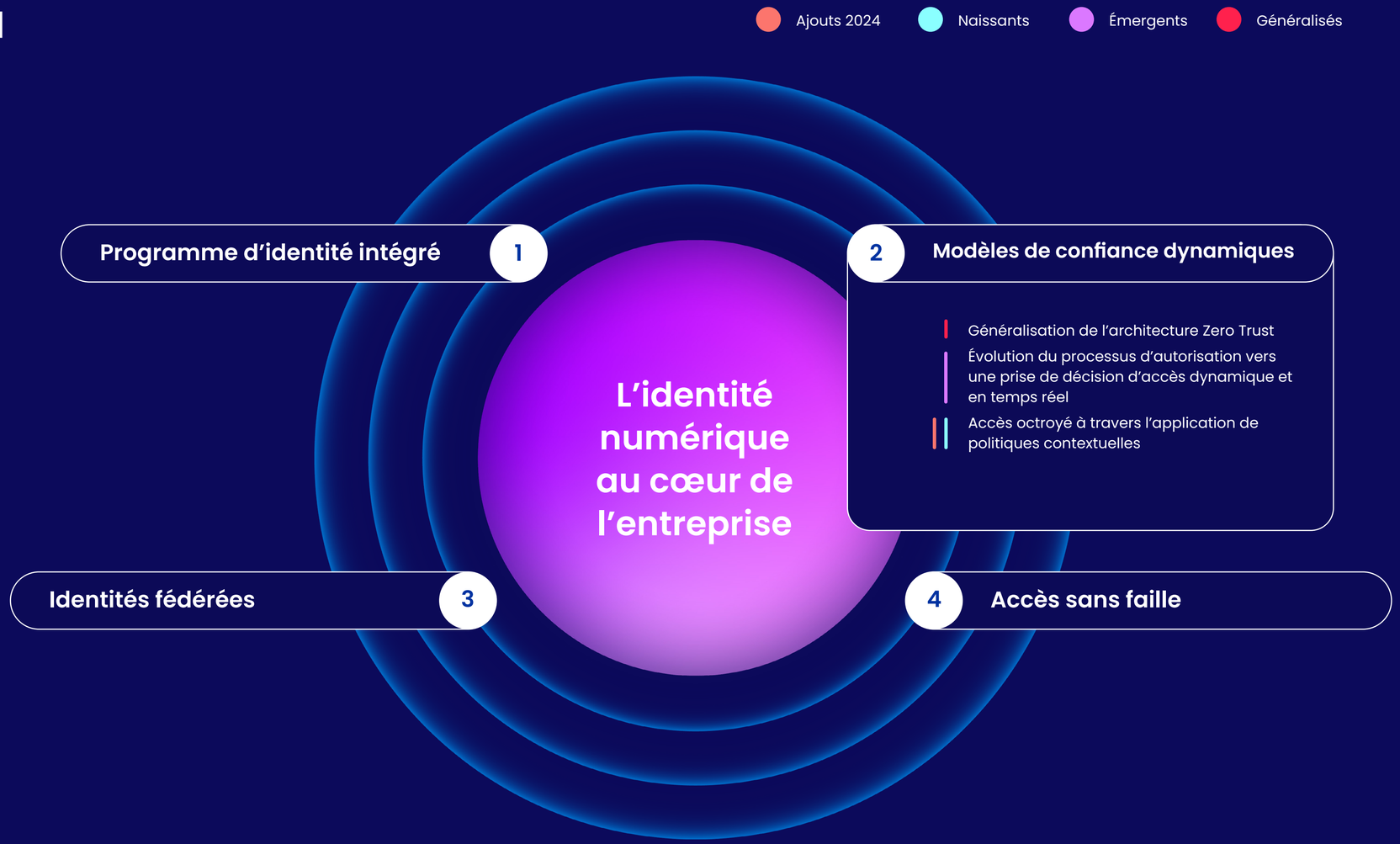
Ces dernières années, nos observations et nos recherches ont confirmé que l'avenir de la sécurité des identités sera façonné par des programmes intégrés de sécurité des identités.

Les principaux éléments sont présentés ici, accompagnés des tendances qui les complètent.

En constante évolution, la réglementation et les risques continuent de façonner ces quatre éléments.

La structure de sécurité des identités deviendra le centre névralgige des futures opérations de sécurité.

La prolifération des réglementations et de normes sectorielles liées à la sécurité des identités, dans le monde entier et dans les différents secteurs d'activité, suscitera des attentes plus fortes en la matière.



L’avenir de l’identité sera régi par 4 éléments clés

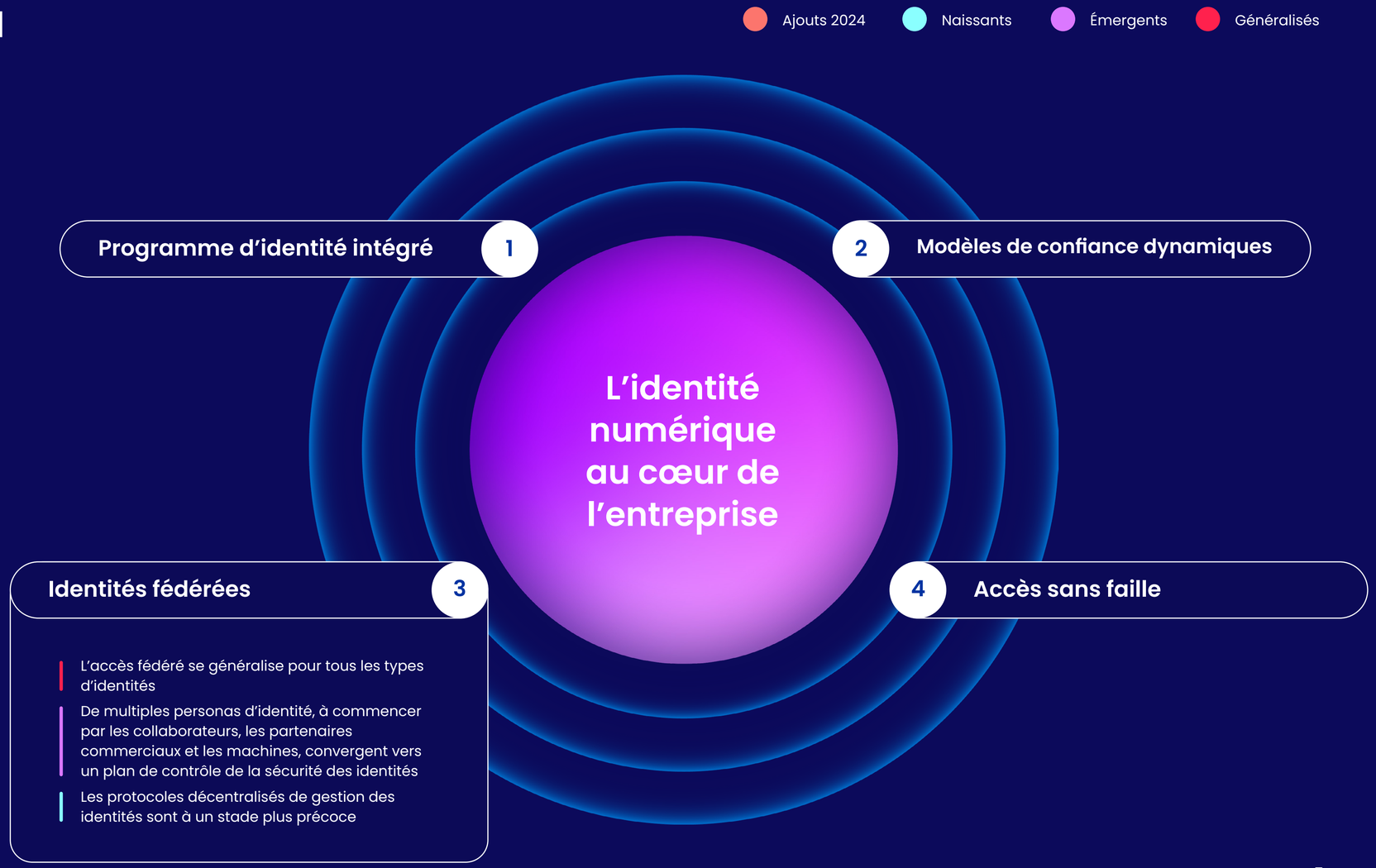
Ces dernières années, nos observations et nos recherches ont confirmé que l’avenir de la sécurité des identités sera façonné par des programmes intégrés de sécurité des identités.

Les principaux éléments sont présentés ici, accompagnés des tendances qui les complètent.

En constante évolution, la réglementation et les risques continuent de façonner ces quatre éléments.

La structure de sécurité des identités deviendra le centre névralgige des futures opérations de sécurité.

La prolifération des réglementations et de normes sectorielles liées à la sécurité des identités, dans le monde entier et dans les différents secteurs d’activité, suscitera des attentes plus fortes en la matière.



L'avenir de l'identité sera régi par 4 éléments clés

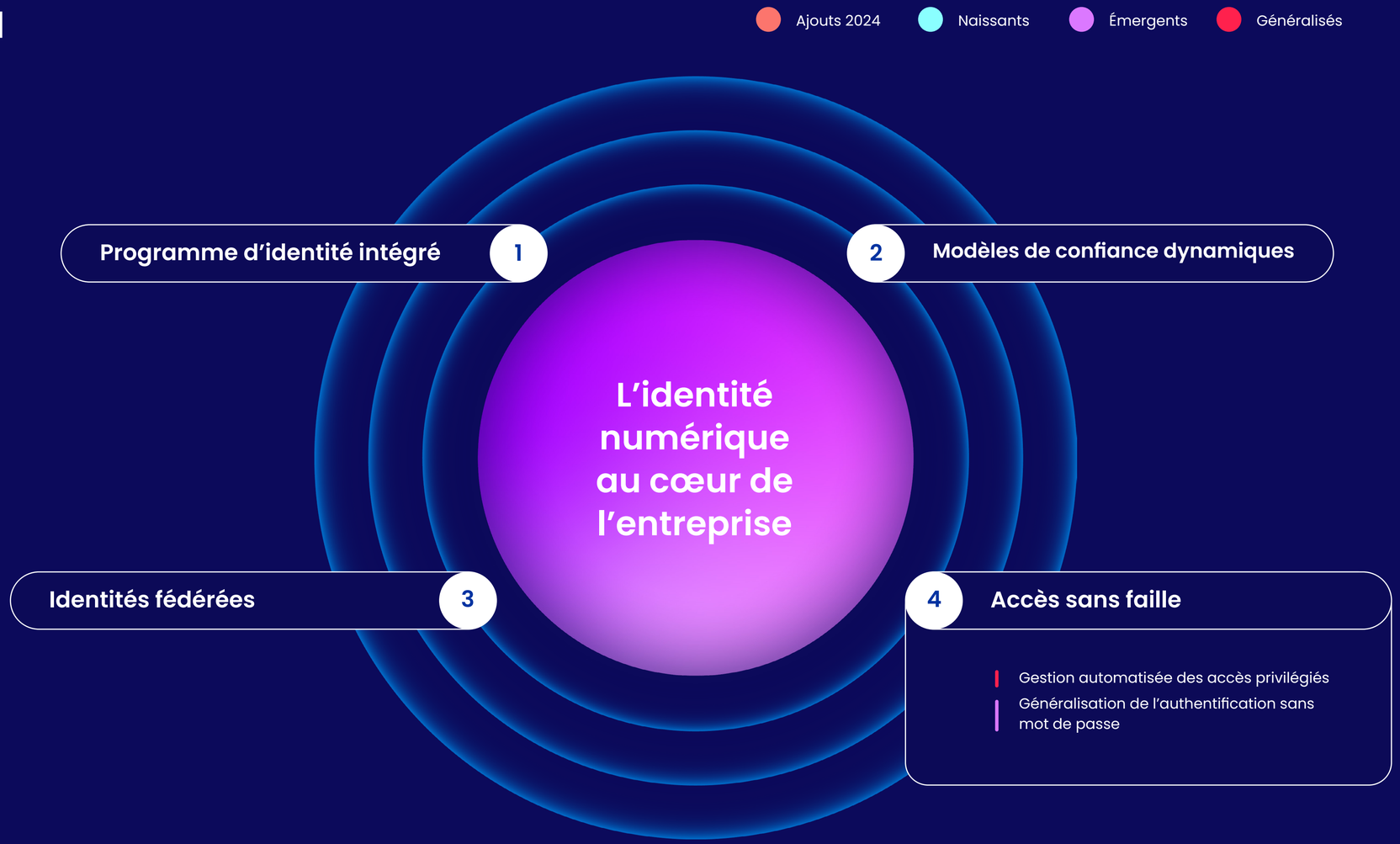
Ces dernières années, nos observations et nos recherches ont confirmé que l'avenir de la sécurité des identités sera façonné par des programmes intégrés de sécurité des identités.

Les principaux éléments sont présentés ici, accompagnés des tendances qui les complètent.

En constante évolution, la réglementation et les risques continuent de façonner ces quatre éléments.

La structure de sécurité des identités deviendra le centre névralgige des futures opérations de sécurité.

La prolifération des réglementations et de normes sectorielles liées à la sécurité des identités, dans le monde entier et dans les différents secteurs d'activité, suscitera des attentes plus fortes en la matière.



CHAPITRE 2

Investir dans la sécurité des identités numériques peut changer la donne

Commencer le chapitre →

Courbe de valeur

Réduction des risques

Valeur commerciale

Productivité

Les entreprises disposant d'une solution mature de sécurité des identités obtiennent des rendements sans commune mesure pour chaque euro investi

Le bond en avant vers les Horizons 3 et 4 a un impact commercial considérable sur la sécurité des identités et permet « d'infléchir la courbe » de manière exponentielle.

*Le diamètre du cercle indique la répartition des horizons

Courbe de valeur

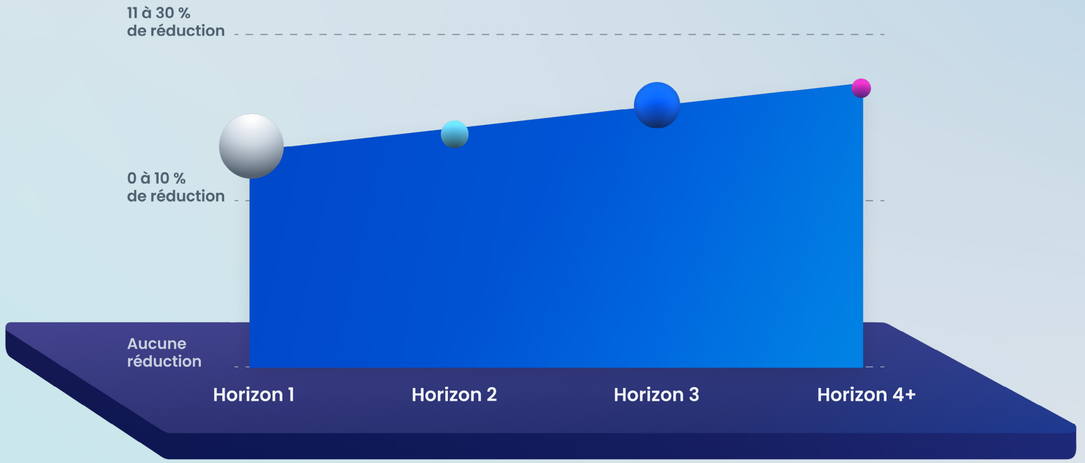
Réduction des risques

Valeur commerciale

Productivité

Le passage d'un horizon de la sécurité des identités au suivant permet de réduire la surface d'attaque pour les violations potentielles

83 % des entreprises font état d'une diminution des problèmes de sécurité liés aux identités du fait de leurs investissements pour mieux les protéger en 2023.



*Le diamètre du cercle indique la répartition des horizons

Courbe de valeur

Réduction des risques

Valeur commerciale

Productivité

Les entreprises dotées de moyens avancés pour sécuriser leurs identités accélèrent leurs lancements de produits et gagnent en efficacité

Chiffre d'affaires en hausse : un niveau avancé de sécurité des identités permet d'accélérer la transformation numérique, favorisant ainsi des cycles de développement plus rapides et une mise sur le marché plus prompte, avec à la clé une croissance du chiffre d'affaires.

*Le diamètre du cercle indique la répartition des horizons

Courbe de valeur

Réduction des risques

Valeur commerciale

Productivité

Les entreprises situées aux Horizons 3, 4 et au-delà sont susceptibles d'enregistrer des gains de productivité considérables

Les entreprises situées à l'Horizon 4 et au-delà constatent d'importants gains de productivité résultant d'une politique intégrée de la sécurité des identités et de l'adoption **de cas d'usage émergents**, tels que les copilotes (conseil), les services (utilisateurs finaux) et l'octroi automatisé des approbations d'accès utilisateurs.

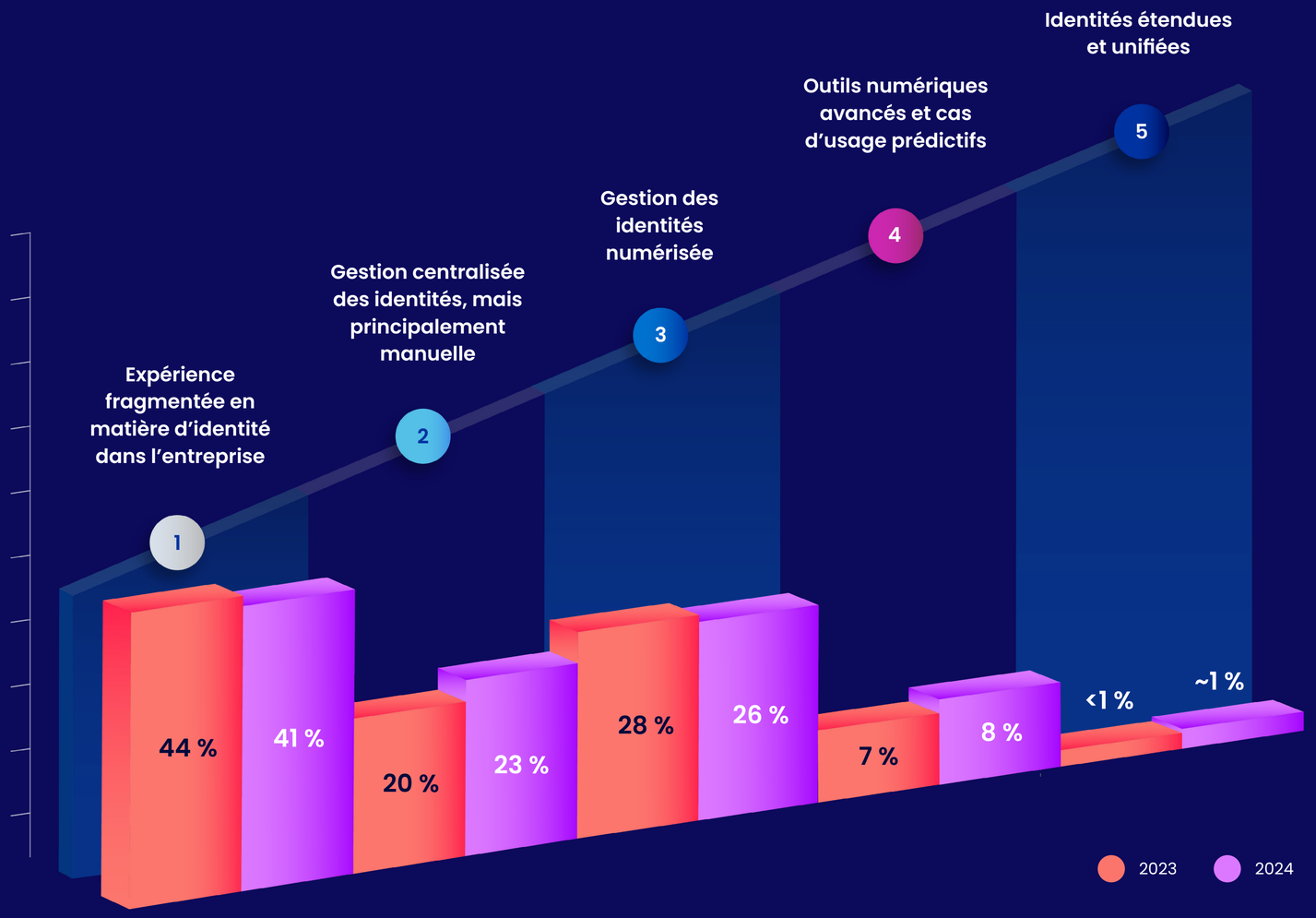
*Le diamètre du cercle indique la répartition des horizons

CHAPITRE 3

Où en sont les entreprises dans leur parcours et pourquoi un niveau de maturité plus élevé leur permettent d'obtenir de meilleurs rendements

Commencer le chapitre →

Étant donné que 41 % des entreprises sont encore situées à l'Horizon 1, il est largement possible d'exploiter pleinement le potentiel de la sécurité des identités



Les entreprises situées à l'Horizon 4 et au-delà réduisent les risques grâce à une couverture de capacités de 70 % sur tous les types d'identités. Les résultats de l'Horizon 3 sont très proches

Les entreprises situées aux Horizons 1 et 2 ont une **couverture des identités très lacunaire.**

Les catégories ci-dessous ne sont actuellement **pas contrôlées.**

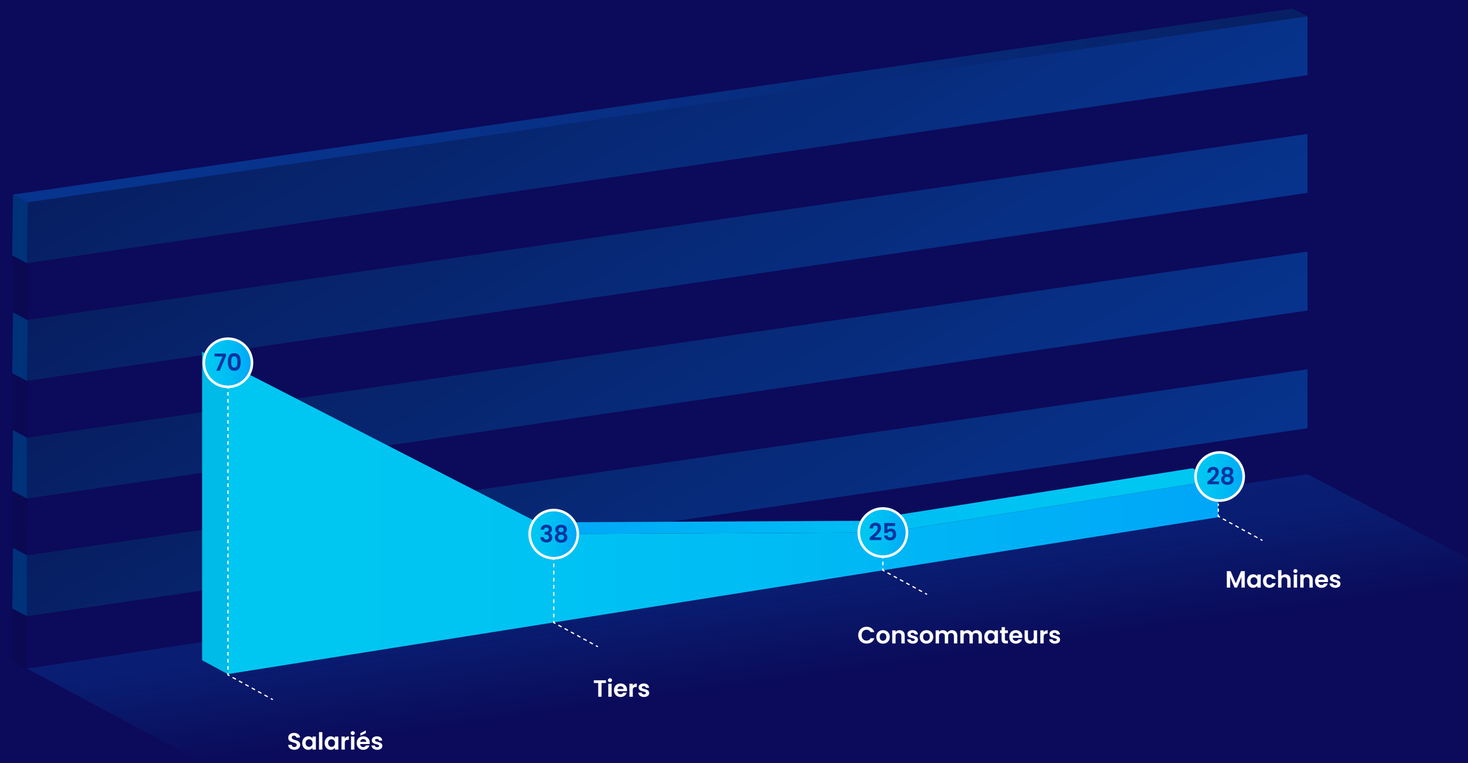
30 % Salariés

62 % Tiers

72 % Identités des machines

Ce dernier point est d'autant plus préoccupant que les identités des mcahines comprennent généralement ~40 à 65 % des identités totales d'une entreprise.

Horizon 1-2 | Horizon 3 | Horizon 4+ | Global | Toutes les données



Les entreprises situées à l'Horizon 4 et au-delà réduisent les risques grâce à une couverture de capacités de 70 % sur tous les types d'identités. Les résultats de l'Horizon 3 sont très proches

Les entreprises situées aux Horizons 1 et 2 ont une **couverture des identités très lacunaire.**

Les catégories ci-dessous ne sont actuellement **pas contrôlées.**

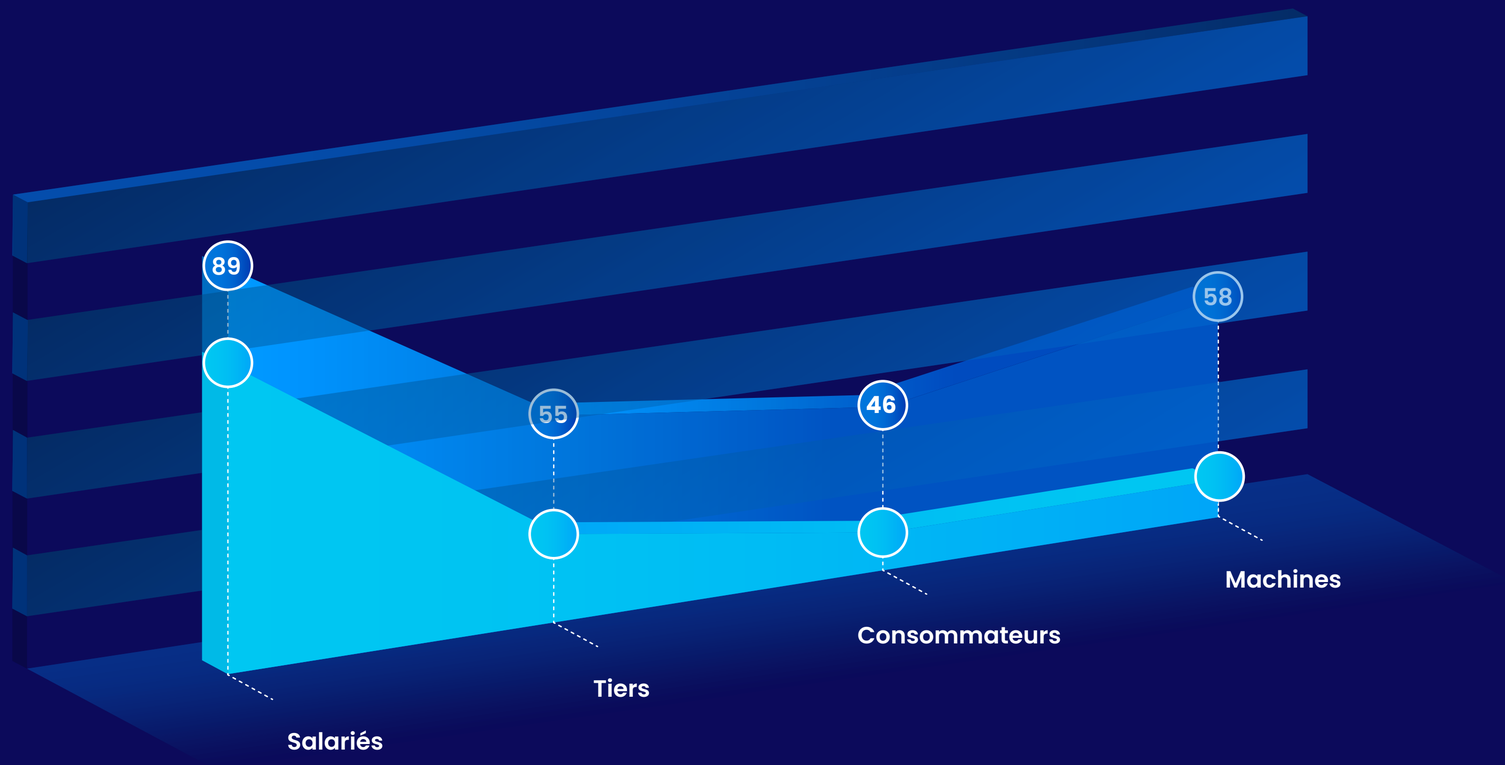
30 % Salariés

62 % Tiers

72 % Identités des machines

Ce dernier point est d'autant plus préoccupant que les identités des mcahines comprennent généralement ~40 à 65 % des identités totales d'une entreprise.

Horizon 1-2 | **Horizon 3** | Horizon 4+ | Global | Toutes les données



Les entreprises situées à l'Horizon 4 et au-delà réduisent les risques grâce à une couverture de capacités de 70 % sur tous les types d'identités. Les résultats de l'Horizon 3 sont très proches

Les entreprises situées aux Horizons 1 et 2 ont une **couverture des identités très lacunaire.**

Les catégories ci-dessous ne sont actuellement **pas contrôlées.**

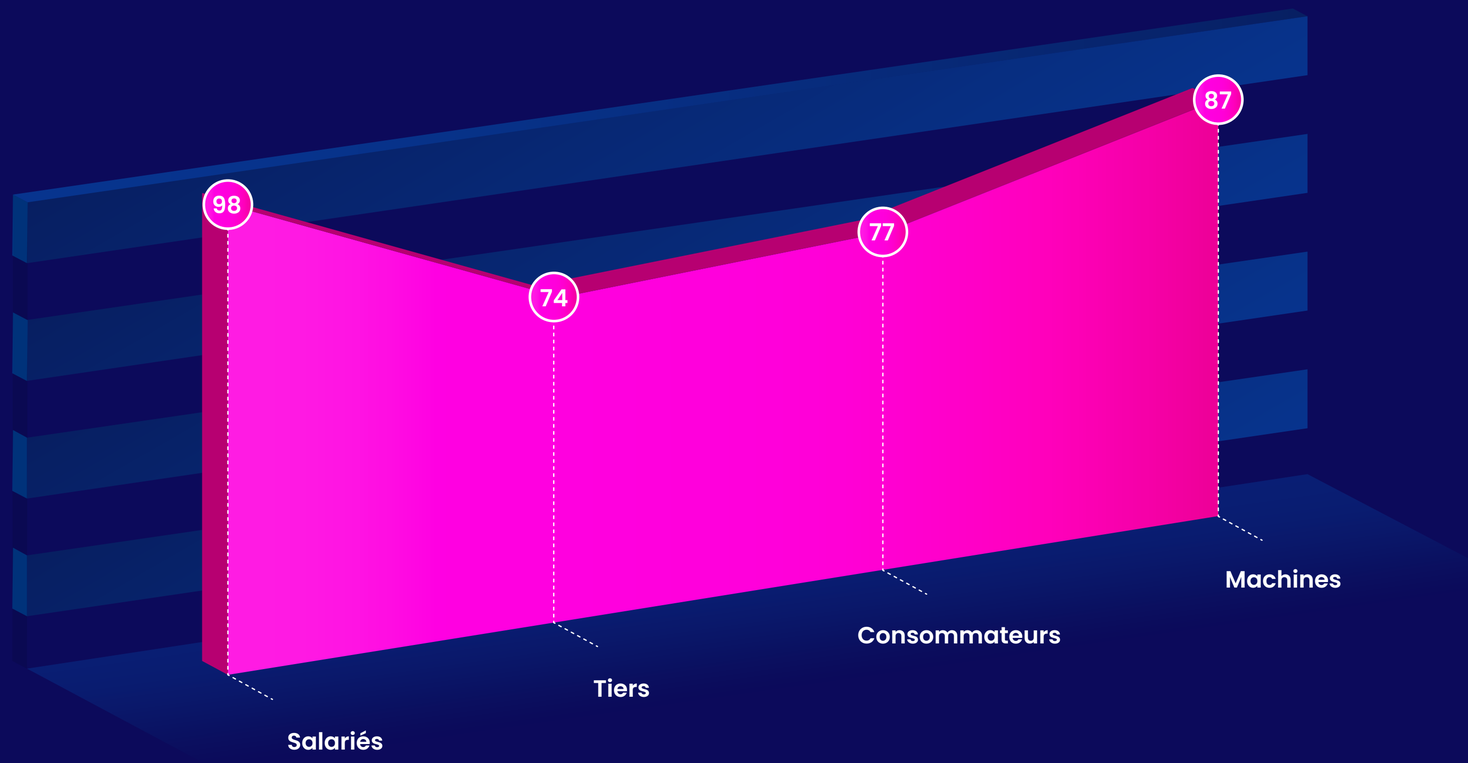
30 % Salariés

62 % Tiers

72 % Identités des machines

Ce dernier point est d'autant plus préoccupant que les identités des mcahines comprennent généralement ~40 à 65 % des identités totales d'une entreprise.

Horizon 1-2 | Horizon 3 | **Horizon 4+** | Global | Toutes les données



Les entreprises situées à l'Horizon 4 et au-delà réduisent les risques grâce à une couverture de capacités de 70 % sur tous les types d'identités. Les résultats de l'Horizon 3 sont très proches

Les entreprises situées aux Horizons 1 et 2 ont une **couverture des identités très lacunaire.**

Les catégories ci-dessous ne sont actuellement **pas contrôlées.**

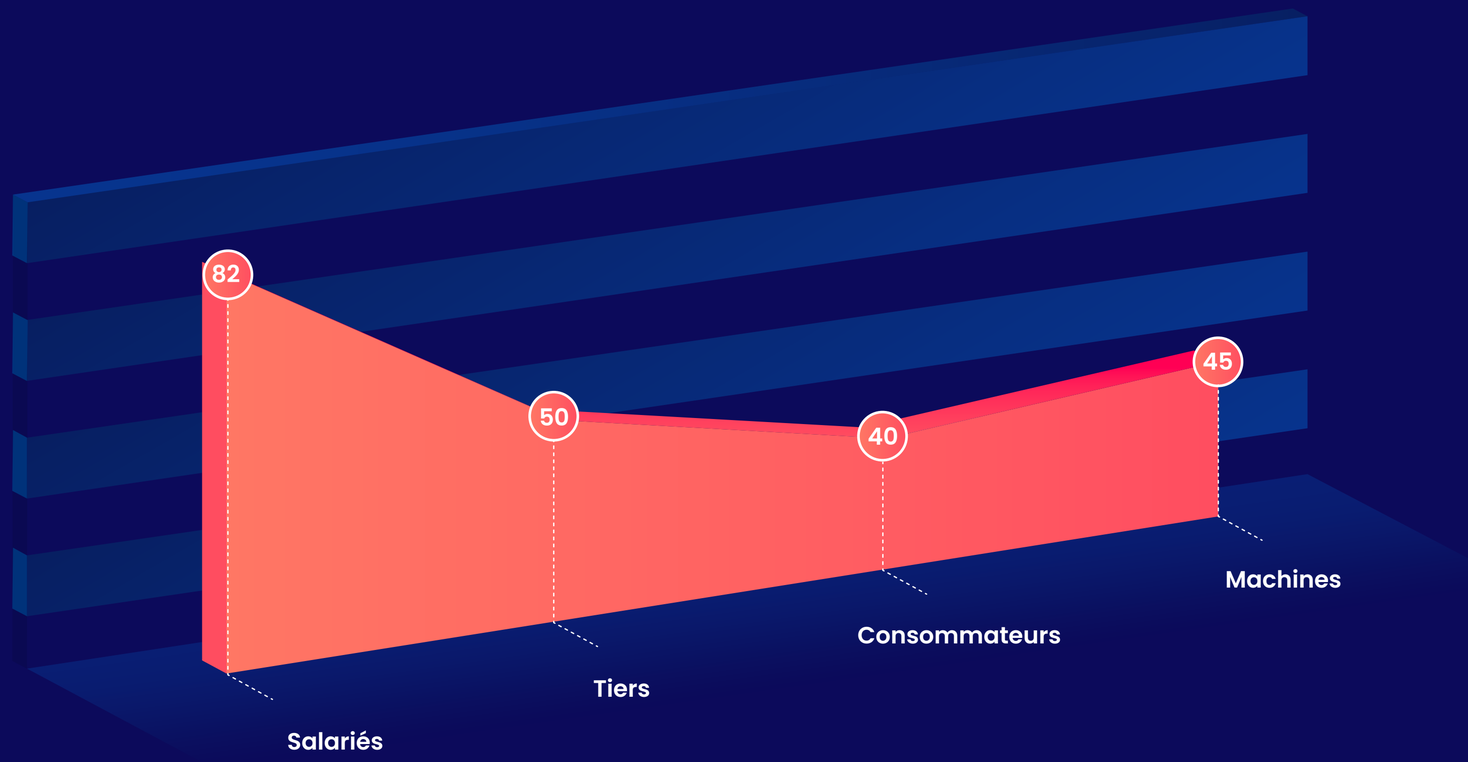
30 % Salariés

62 % Tiers

72 % Identités des machines

Ce dernier point est d'autant plus préoccupant que les identités des mcahines comprennent généralement ~40 à 65 % des identités totales d'une entreprise.

Horizon 1-2 | Horizon 3 | Horizon 4+ | **Global** | Toutes les données



Les entreprises situées à l'Horizon 4 et au-delà réduisent les risques grâce à une couverture de capacités de 70 % sur tous les types d'identités. Les résultats de l'Horizon 3 sont très proches

Les entreprises situées aux Horizons 1 et 2 ont une **couverture des identités très lacunaire.**

Les catégories ci-dessous ne sont actuellement **pas contrôlées.**

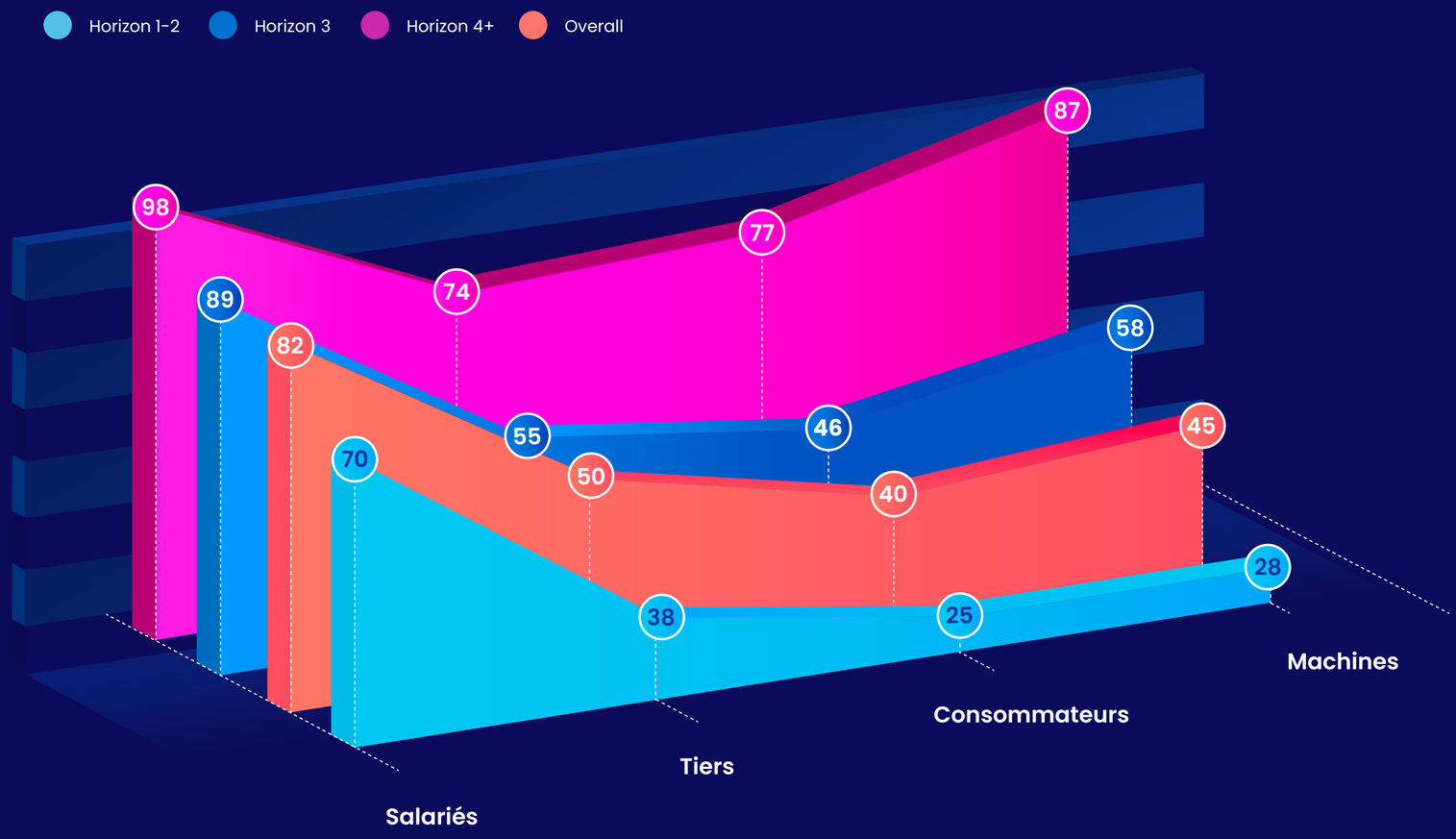
30 % Salariés

62 % Tiers

72 % Identités des machines

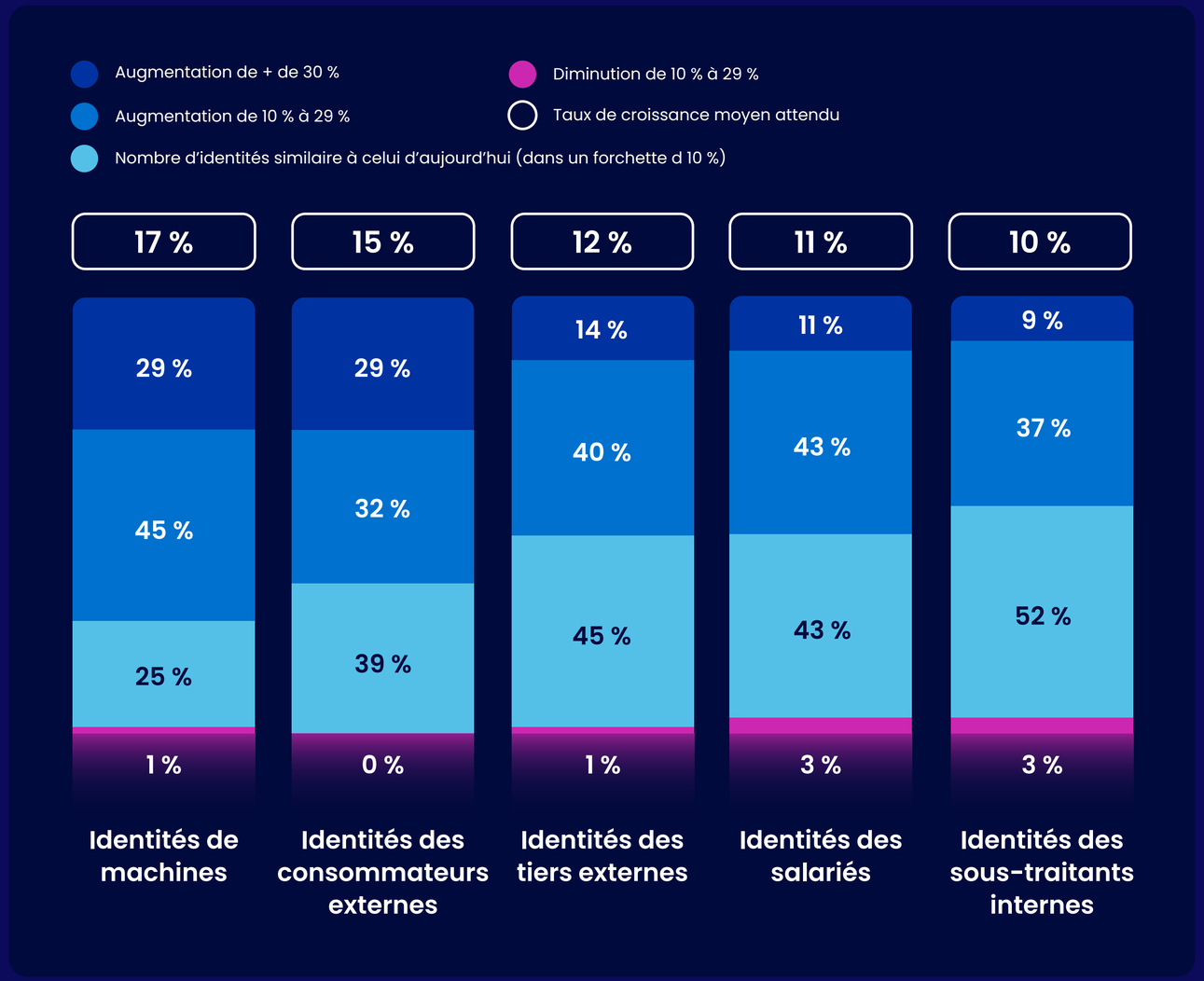
Ce dernier point est d'autant plus préoccupant que les identités des mcahines comprennent généralement ~40 à 65 % des identités totales d'une entreprise.

Horizon 1-2 | Horizon 3 | Horizon 4+ | Overall | **Toutes les donées**

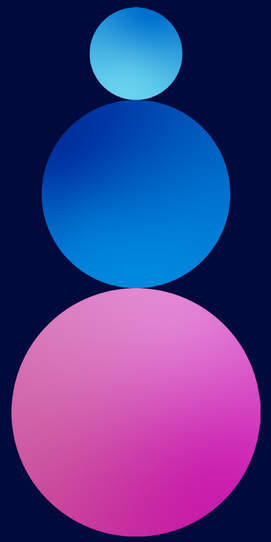


Une croissance d'environ 14 % de l'ensemble des identités est attendue au cours des 3 à 5 prochaines années, mais ce sont les identités des machines qui connaîtront la croissance la plus rapide

La croissance des **identités des machines** pourrait dépasser celle des identités humaines.



Les entreprises situées à l'Horizon 4 et au-delà sont deux fois plus susceptibles de tirer parti des données d'identité pour produire des renseignements exploitables et des nouveaux cas d'usage



<20 %

des entreprises situées aux Horizons 1 et 2 exploitent à grande échelle les données de cyberveille relatives aux identités

<40 %

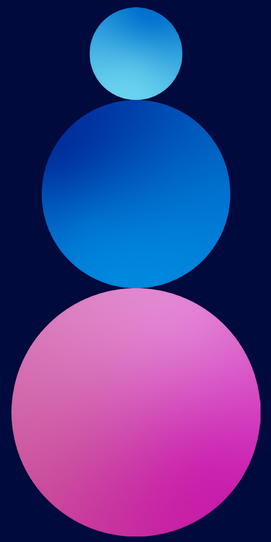
des entreprises situées à l'Horizon 3 exploitent à grande échelle les données de cyberveille relatives aux identités

~50 %

des entreprises situées à l'Horizon 4 et au-delà utilisent les recommandations intelligentes tirées des données structurées et non-structurées en ce qui concerne l'accès des utilisateurs, les politiques de sécurité et les examens d'accès

Horizon 1-2 | Horizon 3 | Horizon 4+ | Global | Toutes les données

Les entreprises situées à l'Horizon 4 et au-delà sont deux fois plus susceptibles de tirer parti des données d'identité pour produire des renseignements exploitables et des nouveaux cas d'usage



<20 %

des entreprises situées aux Horizons 1 et 2 exploitent à grande échelle les données de cyberveille relatives aux identités

<40 %

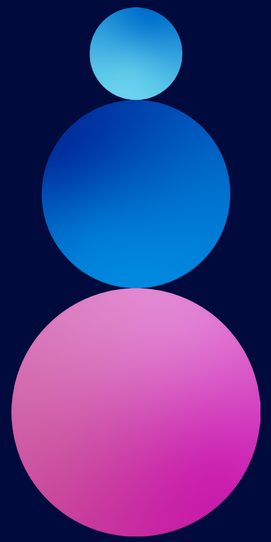
des entreprises situées à l'Horizon 3 exploitent à grande échelle les données de cyberveille relatives aux identités

~50 %

des entreprises situées à l'Horizon 4 et au-delà utilisent les recommandations intelligentes tirées des données structurées et non-structurées en ce qui concerne l'accès des utilisateurs, les politiques de sécurité et les examens d'accès

Horizon 1-2 | Horizon 3 | Horizon 4+ | Global | Toutes les données

Les entreprises situées à l'Horizon 4 et au-delà sont deux fois plus susceptibles de tirer parti des données d'identité pour produire des renseignements exploitables et des nouveaux cas d'usage



<20 %

des entreprises situées aux Horizons 1 et 2 exploitent à grande échelle les données de cyberveille relatives aux identités

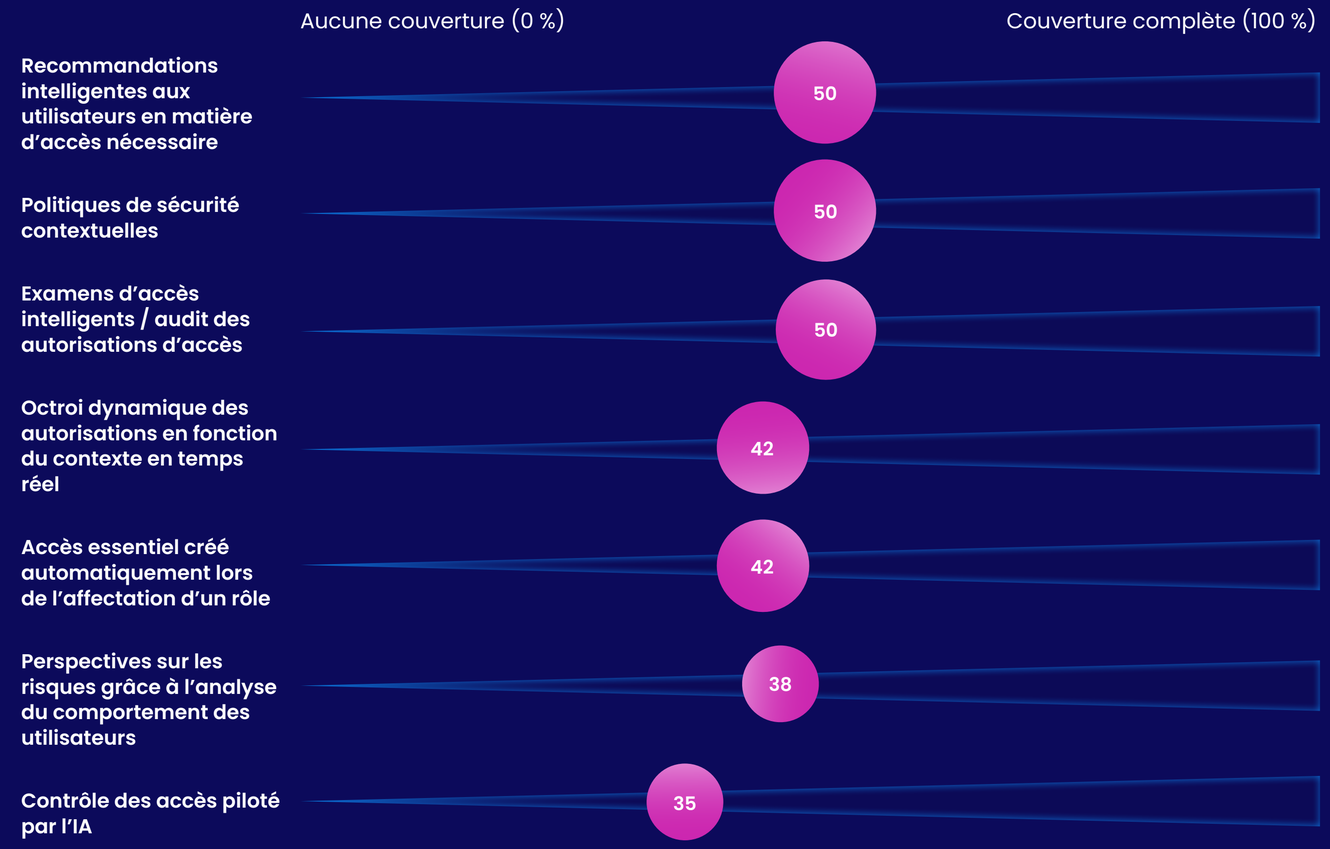
<40 %

des entreprises situées à l'Horizon 3 exploitent à grande échelle les données de cyberveille relatives aux identités

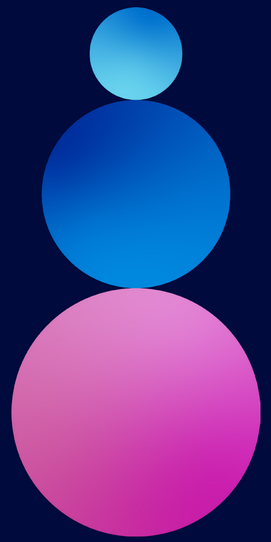
~50 %

des entreprises situées à l'Horizon 4 et au-delà utilisent les recommandations intelligentes tirées des données structurées et non-structurées en ce qui concerne l'accès des utilisateurs, les politiques de sécurité et les examens d'accès

Horizon 1-2 | Horizon 3 | Horizon 4+ | Global | Toutes les données



Les entreprises situées à l'Horizon 4 et au-delà sont deux fois plus susceptibles de tirer parti des données d'identité pour produire des renseignements exploitables et des nouveaux cas d'usage



<20 %

des entreprises situées aux Horizons 1 et 2 exploitent à grande échelle les données de cyberveille relatives aux identités

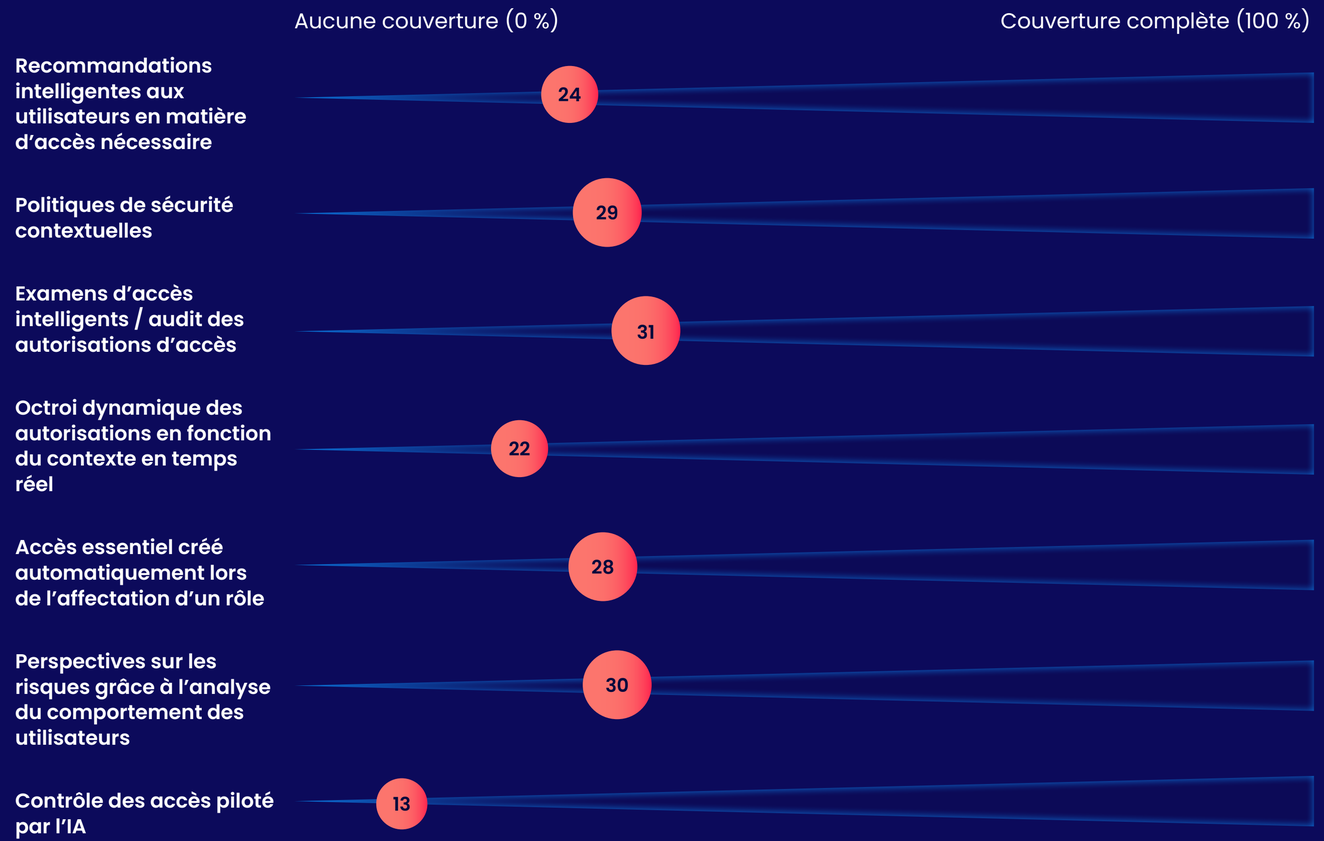
<40 %

des entreprises situées à l'Horizon 3 exploitent à grande échelle les données de cyberveille relatives aux identités

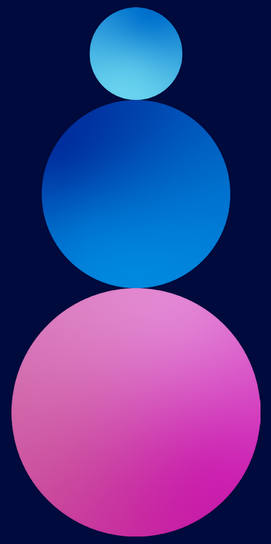
~50 %

des entreprises situées à l'Horizon 4 et au-delà utilisent les recommandations intelligentes tirées des données structurées et non-structurées en ce qui concerne l'accès des utilisateurs, les politiques de sécurité et les examens d'accès

Horizon 1-2 | Horizon 3 | Horizon 4+ | **Global** | Toutes les données



Les entreprises situées à l'Horizon 4 et au-delà sont deux fois plus susceptibles de tirer parti des données d'identité pour produire des renseignements exploitables et des nouveaux cas d'usage



<20 %

des entreprises situées aux Horizons 1 et 2 exploitent à grande échelle les données de cyberveille relatives aux identités

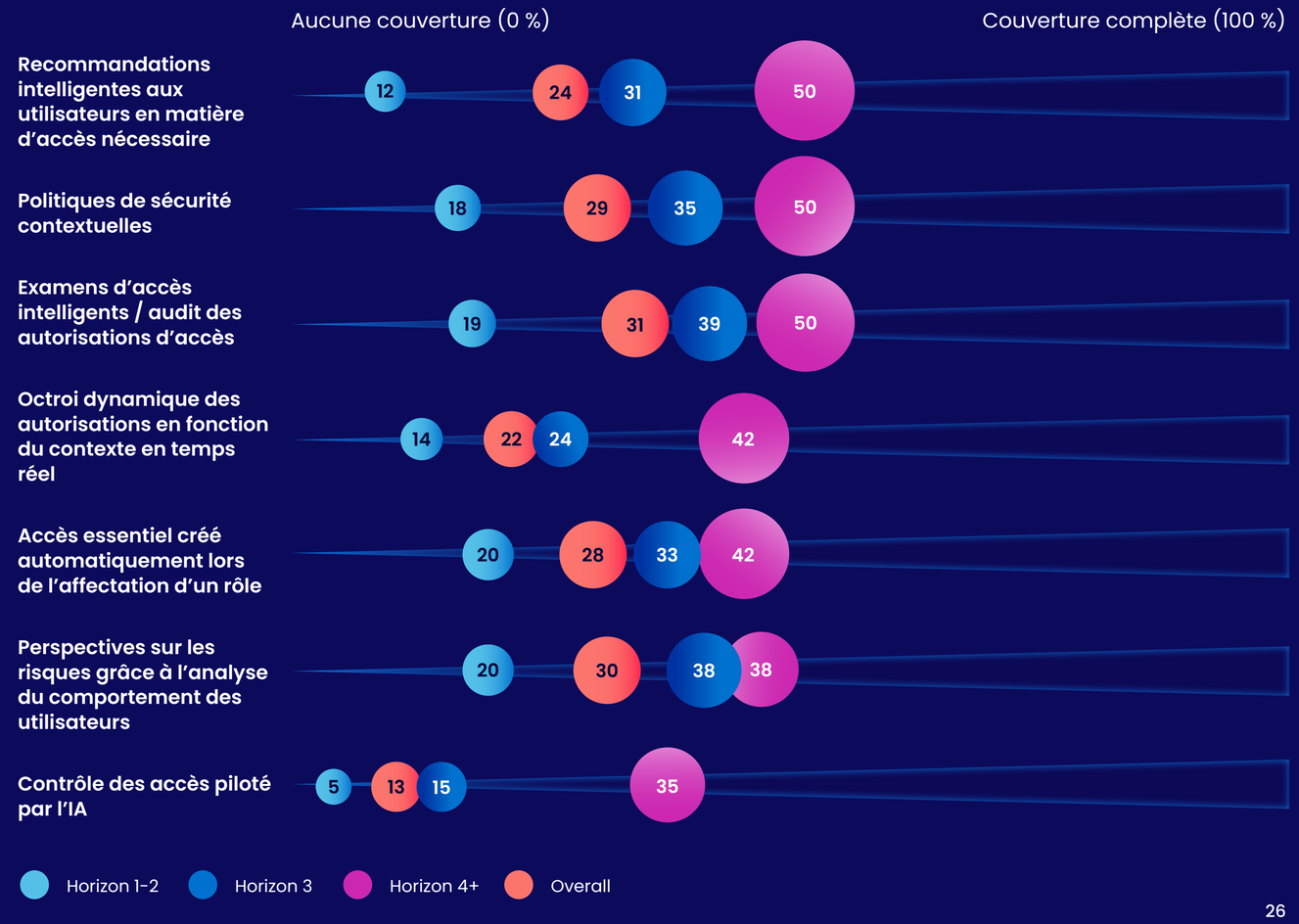
<40 %

des entreprises situées à l'Horizon 3 exploitent à grande échelle les données de cyberveille relatives aux identités

~50 %

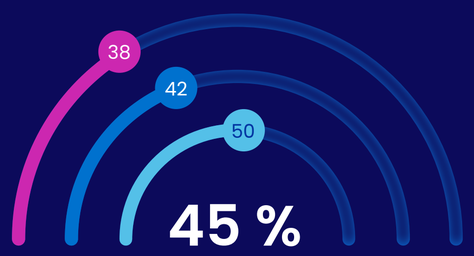
des entreprises situées à l'Horizon 4 et au-delà utilisent les recommandations intelligentes tirées des données structurées et non-structurées en ce qui concerne l'accès des utilisateurs, les politiques de sécurité et les examens d'accès

Horizon 1-2 | Horizon 3 | Horizon 4+ | Overall | **Toutes les données**

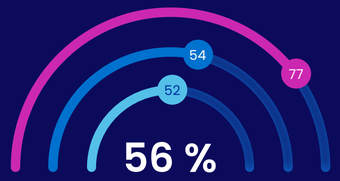


Les entreprises disposant d'une solution mature de sécurité des identités sont en mesure d'investir dans des cas d'usage évolutifs basés sur l'IA générative

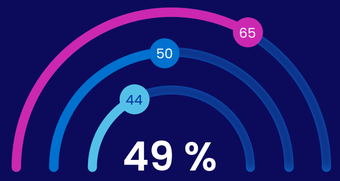
Les entreprises situées à l'Horizon 3 et au-delà se concentrent sur la conception de solutions évolutives afin d'augmenter et d'étendre la sécurité de leurs identités. Tandis que les entreprises situées aux Horizons 1 et 2 mettent l'accent sur l'automatisation des activités répétitives de type service d'assistance.



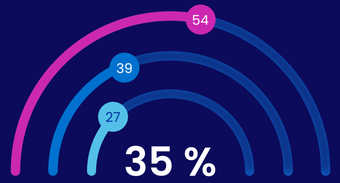
Robots conversationnels d'IA offrant une assistance instantanée en matière d'IAM et de gestion des tâches



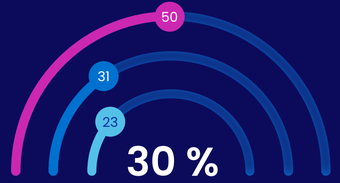
Création de flux de travail formulés par l'IA (y compris provisioning des utilisateurs, examens d'accès et gestion des rôles)



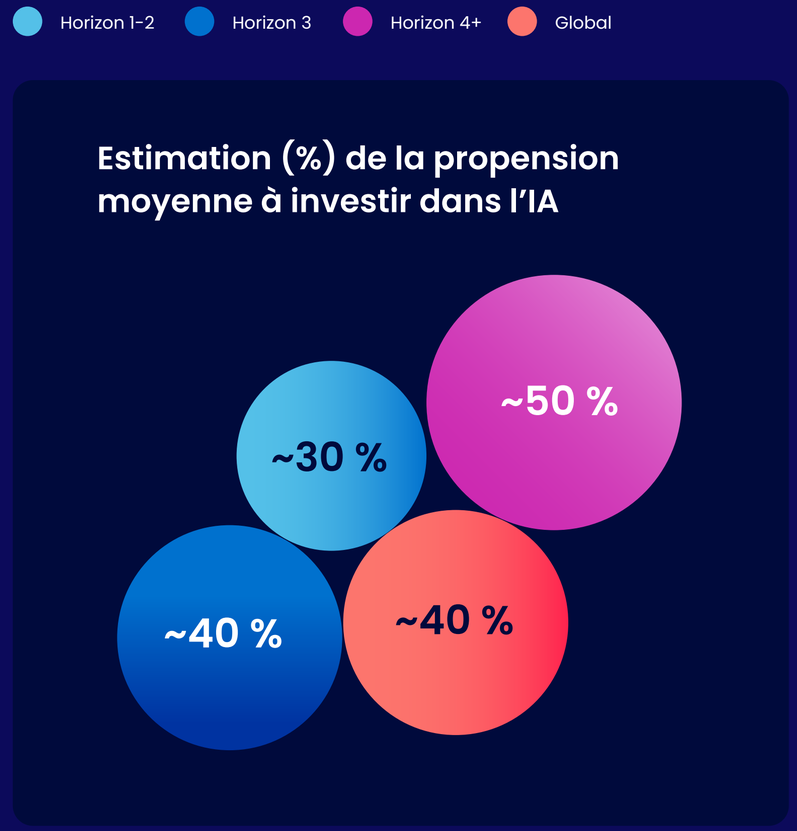
Descriptions des rôles et droits des utilisateurs générées par l'IA (y compris les droits, les privilèges et les niveaux d'accès)



Recherche en langage naturel facilitant l'extraction des données IAM



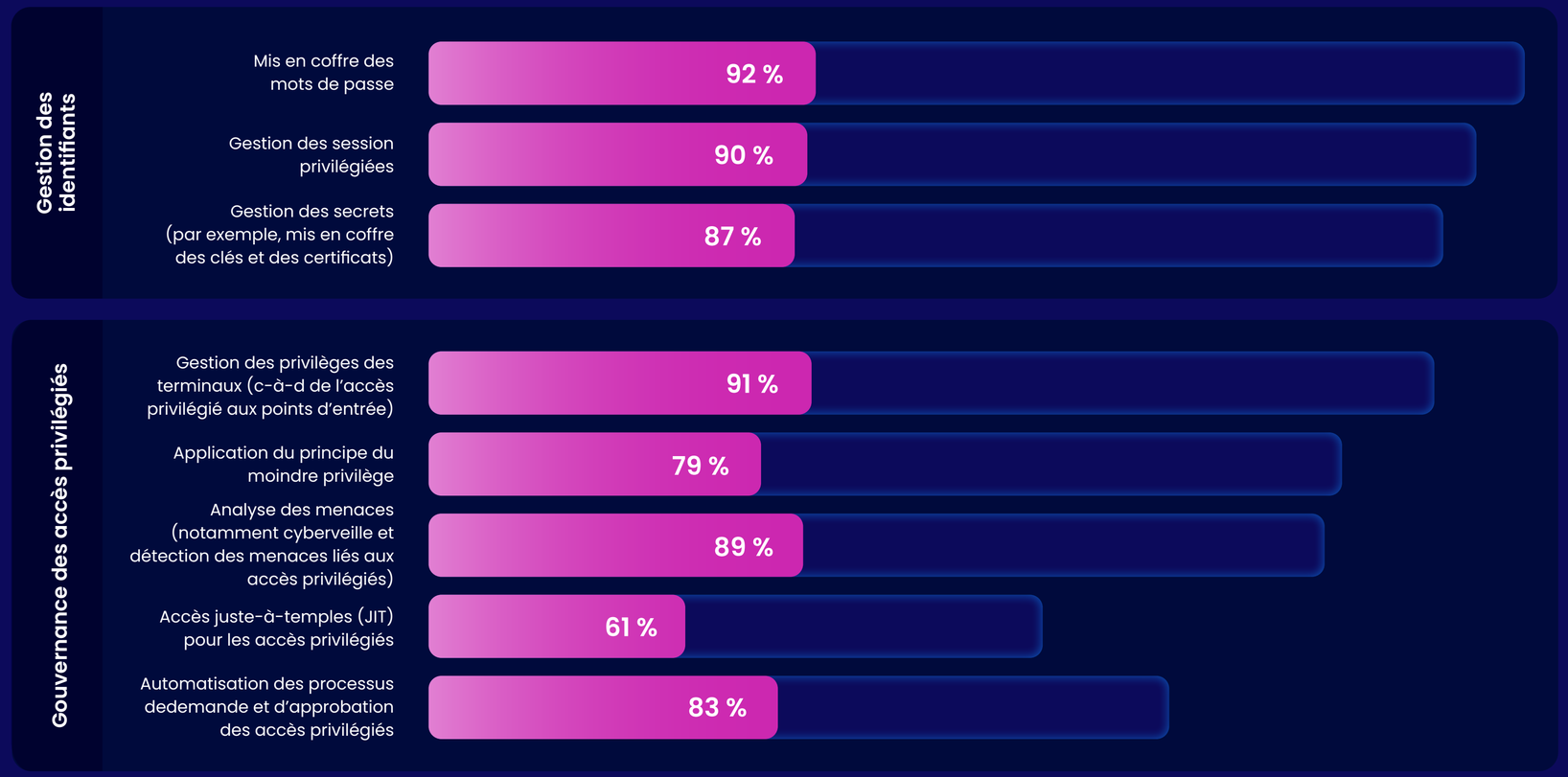
Copilotes pour le développement automatisé de connecteurs



Les entreprises situées à l'Horizon 3 et au-delà affichent un taux d'adoption des capacités de gouvernance des accès privilégiés jusqu'à 50 % supérieur à celui des entreprises des Horizons 1 et 2

En investissant dans des solutions qui vont au-delà de la gestion des sessions et de la mise en coffre des identifiants, les entreprises peuvent simplifier les processus de demande et d'approbation des accès, tout en améliorant l'analyse des menaces pour les comptes privilégiés.

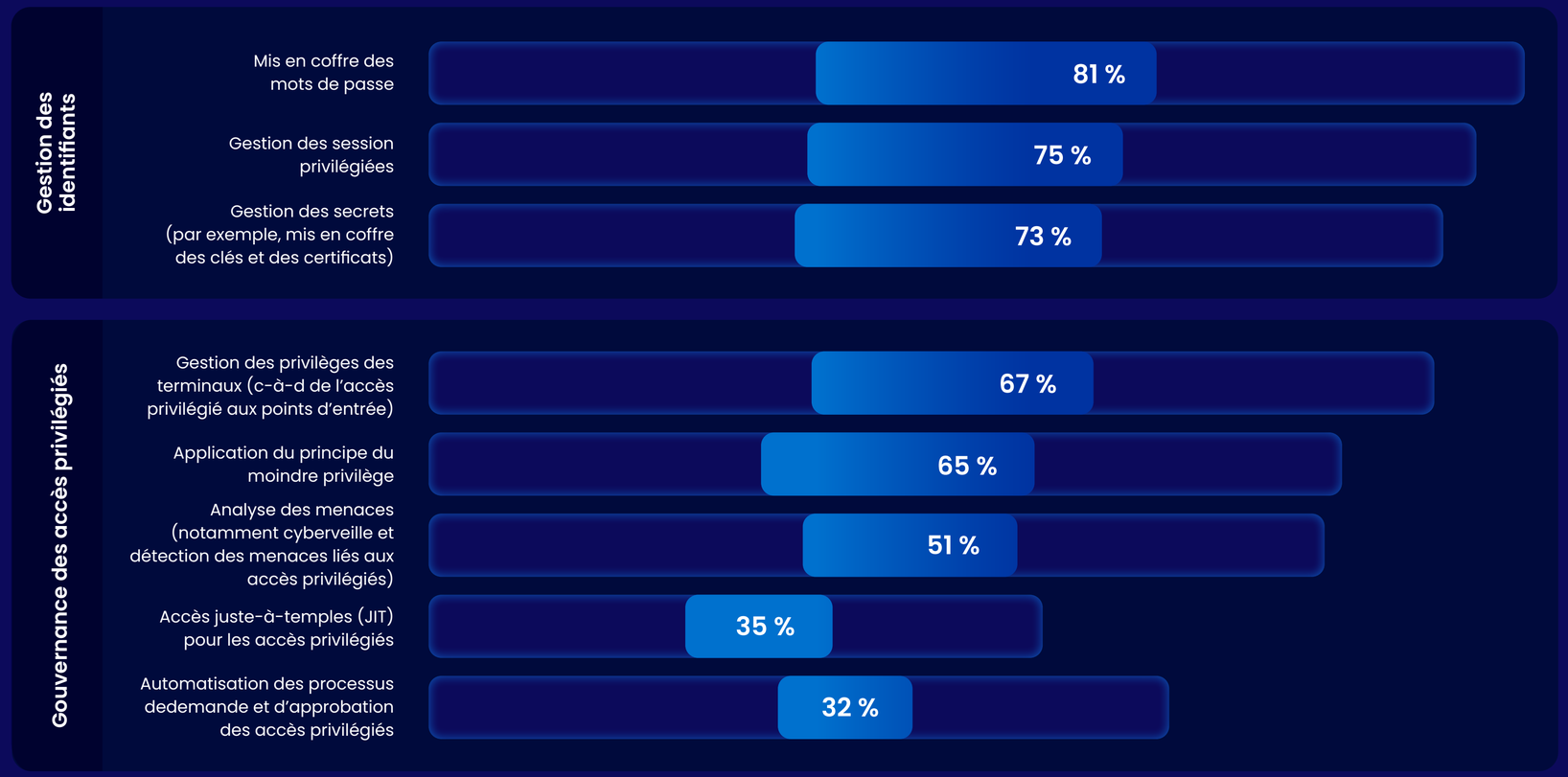
Horizon 3+ | Horizon 1-2 | Global | Données



Les entreprises situées à l'Horizon 3 et au-delà affichent un taux d'adoption des capacités de gouvernance des accès privilégiés jusqu'à 50 % supérieur à celui des entreprises des Horizons 1 et 2

En investissant dans des solutions qui vont au-delà de la gestion des sessions et de la mise en coffre des identifiants, les entreprises peuvent simplifier les processus de demande et d'approbation des accès, tout en améliorant l'analyse des menaces pour les comptes privilégiés.

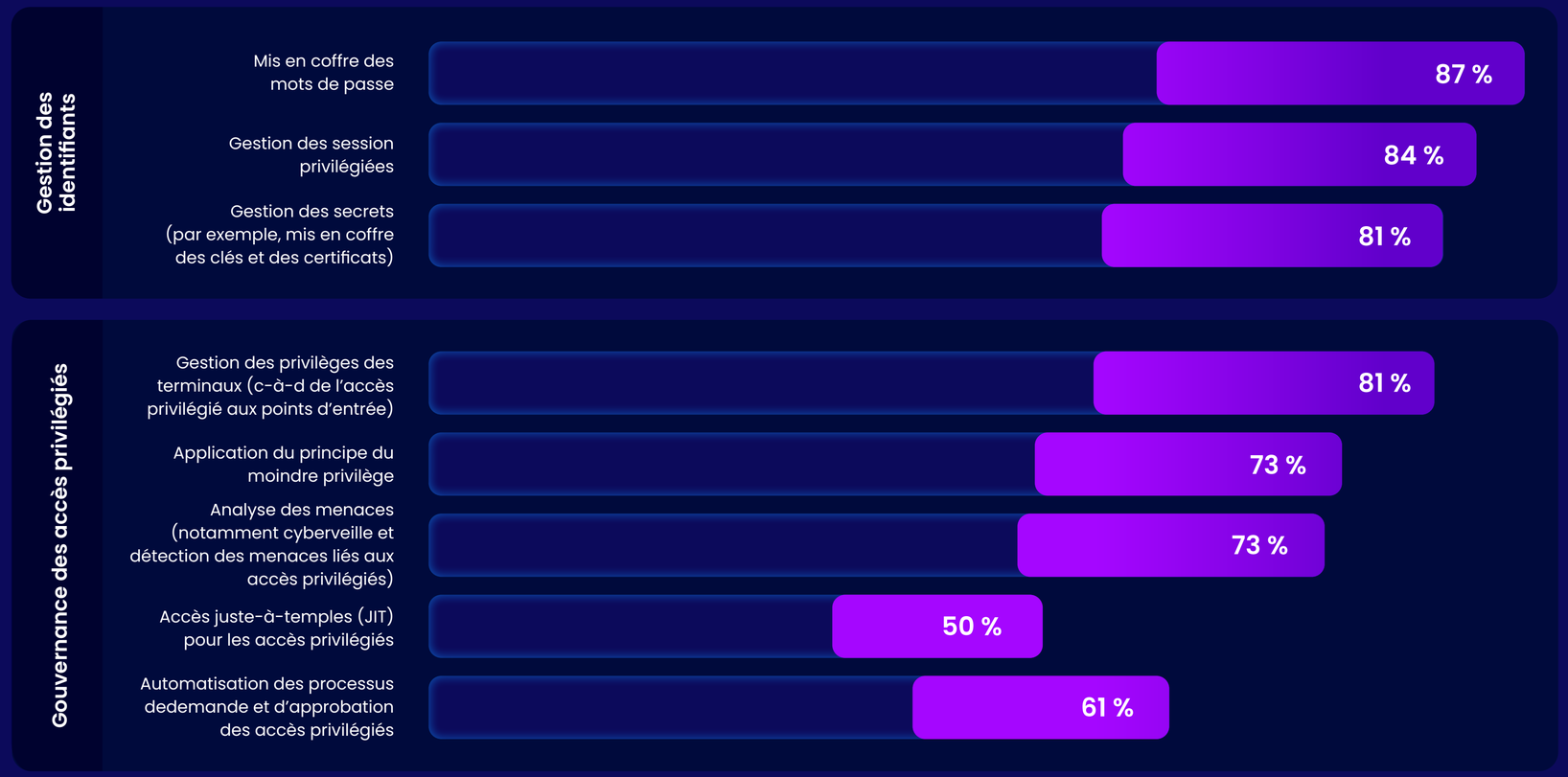
Horizon 3+ | Horizon 1-2 | Global | Données



Les entreprises situées à l'Horizon 3 et au-delà affichent un taux d'adoption des capacités de gouvernance des accès privilégiés jusqu'à 50 % supérieur à celui des entreprises des Horizons 1 et 2

En investissant dans des solutions qui vont au-delà de la gestion des sessions et de la mise en coffre des identifiants, les entreprises peuvent simplifier les processus de demande et d'approbation des accès, tout en améliorant l'analyse des menaces pour les comptes privilégiés.

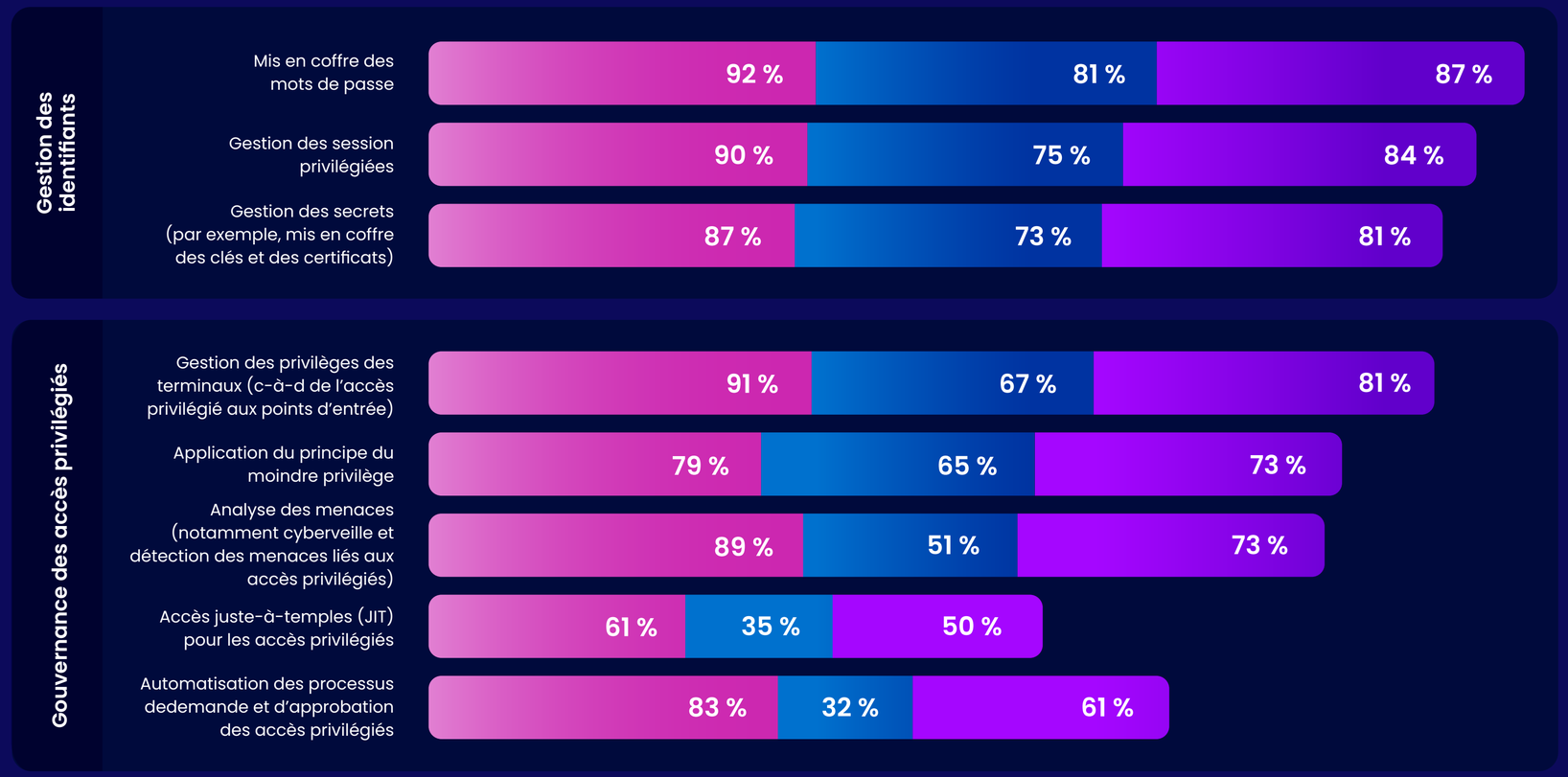
Horizon 3+ | Horizon 1-2 | Global | Données



Les entreprises situées à l'Horizon 3 et au-delà affichent un taux d'adoption des capacités de gouvernance des accès privilégiés jusqu'à 50 % supérieur à celui des entreprises des Horizons 1 et 2

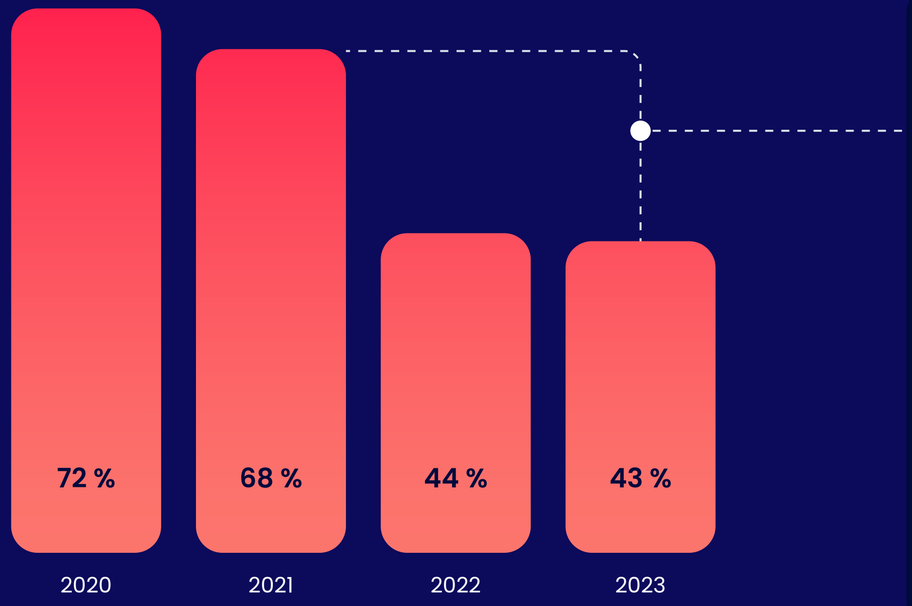
En investissant dans des solutions qui vont au-delà de la gestion des sessions et de la mise en coffre des identifiants, les entreprises peuvent simplifier les processus de demande et d'approbation des accès, tout en améliorant l'analyse des menaces pour les comptes privilégiés.

Horizon 3+ | Horizon 1-2 | Global | Données



L'amélioration des méthodes de calcul utilisées par les cyber-assureurs pour évaluer la gestion du risque cyber a eu pour conséquence d'augmenter les primes d'assurance cyber.

Les cyber-assureurs ont réduit leur taux de sinistres, acquis de la maturité dans l'évaluation et la gestion des risques . . .

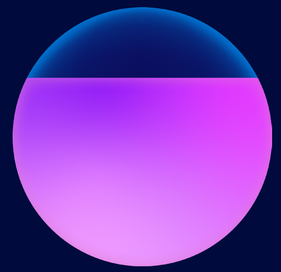


Taux de sinistres propres à la couverture du risque cyber, part des primes versées au titre des sinistres.

40 %

La réduction de la sinistralité chez les cyber-assureurs témoigne d'une meilleure gestion du risque cyber

. . . et ont augmenté leurs primes en fonction du profil de risque accru.



77 %

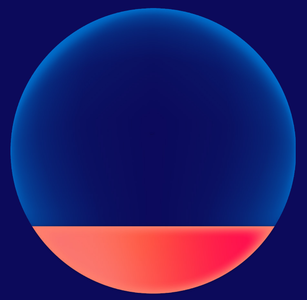
Les entreprises font état d'augmentations de primes au cours des 3 dernières années

“

Les cyber assureurs s’intéressent de plus en plus aux contrôles de sécurité mis en place par les entreprises… ils peuvent même proposer des remises pour renforcer ces contrôles.

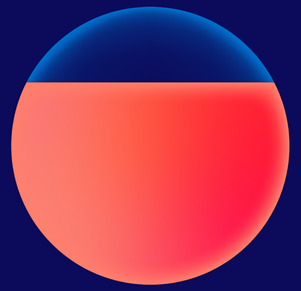
Un professionnel de l’assurance cyber d’une grande société de courtage

Les assurés contre les risques cyber déclarent que les capacités de sécurité des identités sont celles qui impactent le plus les évaluations réalisées par les assureurs



25 %

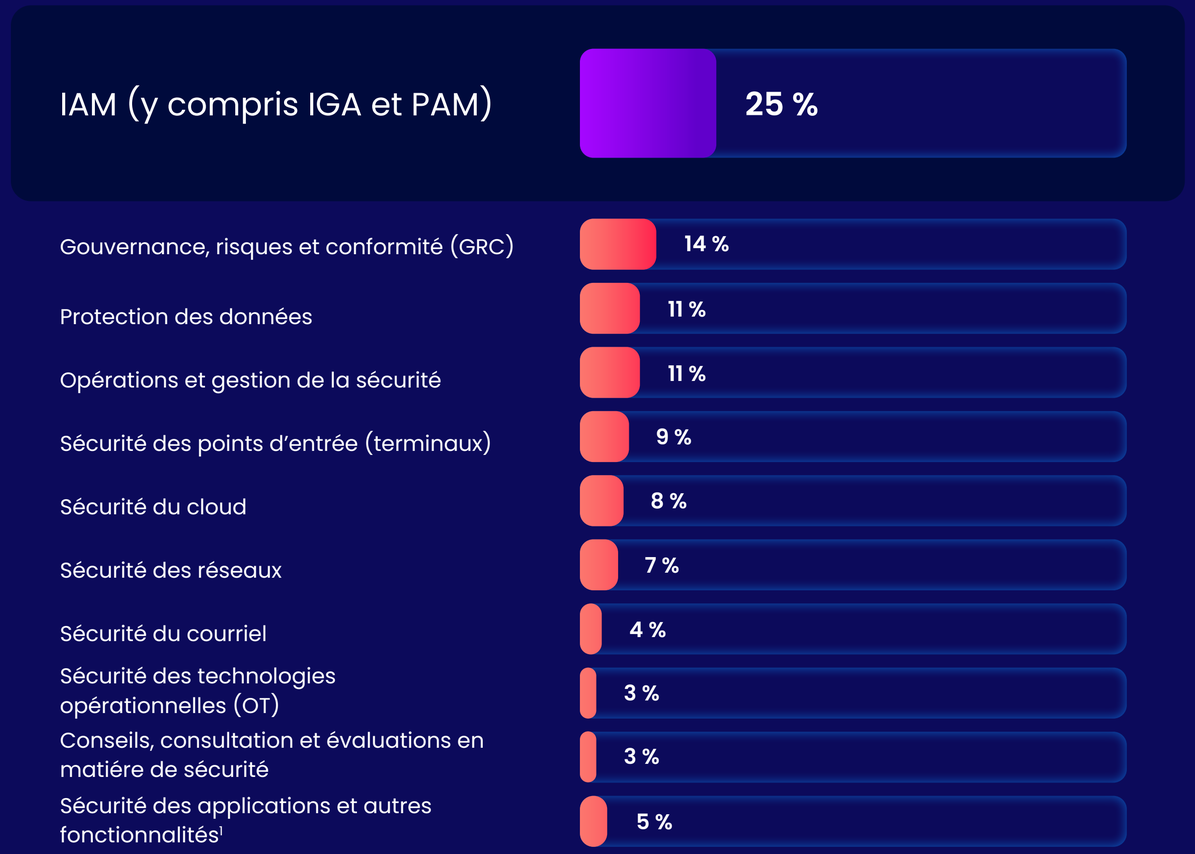
des répondants considèrent l'IAM comme l'élément le plus décisif en ce qui concerne les primes d'assurance contre les risques cyber, c'est la plus grande proportion



73 %

des assurés contre les risques cyber considèrent l'IAM comme l'une des trois principales capacités

Principales capacités de cybersécurité impactant les évaluations réalisées au titre de l'assurance des risques cyber, pourcentage de répondants indiquant que cette capacité est la plus décisive de toutes.



[1] Inclut la sécurité web, les fournisseurs MSSP et l'externalisation

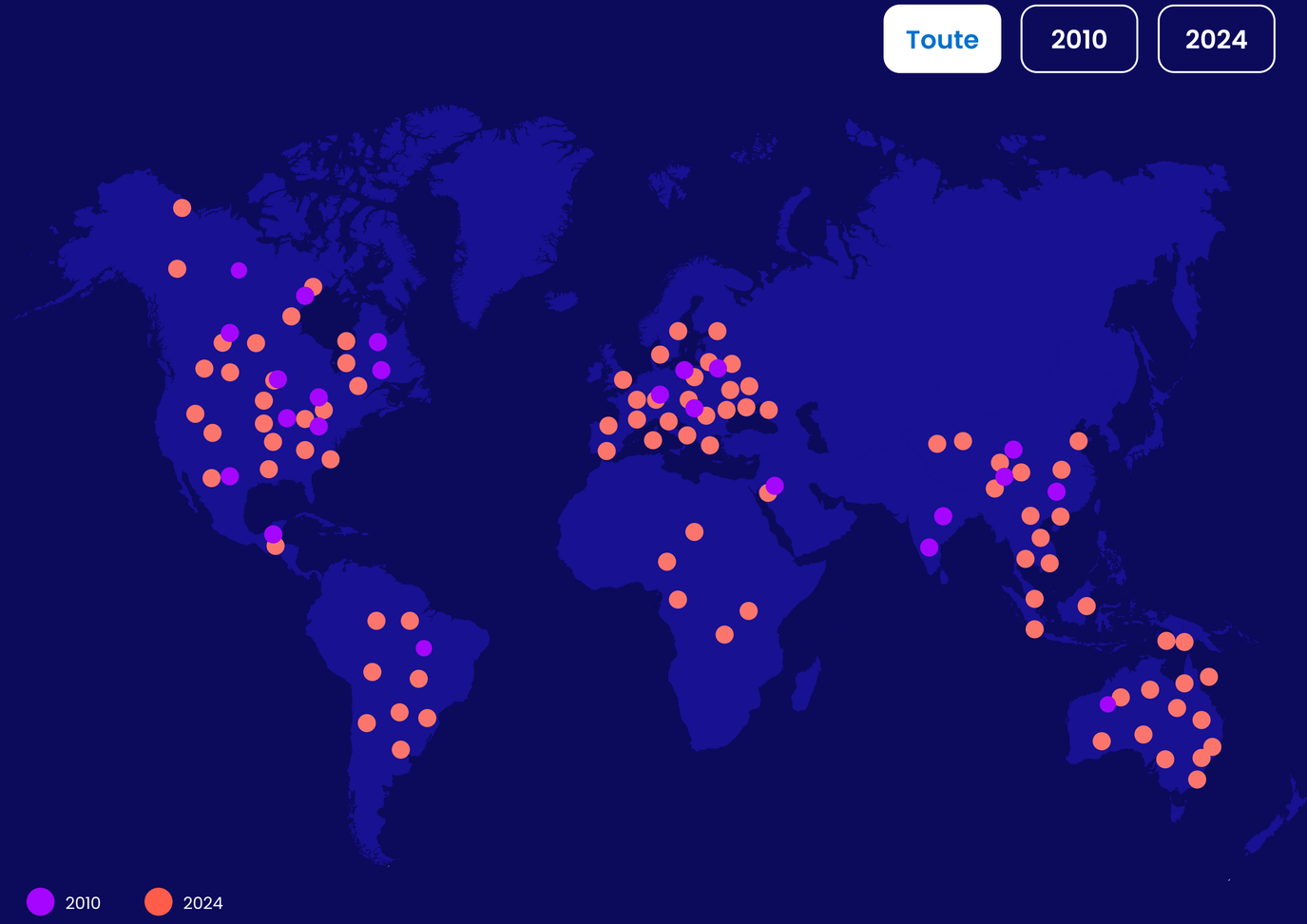
Le nombre de réglementations relatives aux identités numériques a été multiplié par 7 depuis 2010 dans toutes les zones géographiques, tous secteurs d'activité confondus

+ de 5 fois plus

de réglementations dans les secteurs autres que la finance et la santé

+ de 13 fois plus

de réglementations en dehors de l'Europe, de l'Amérique du Nord, et de la zone Asie-Pacifique

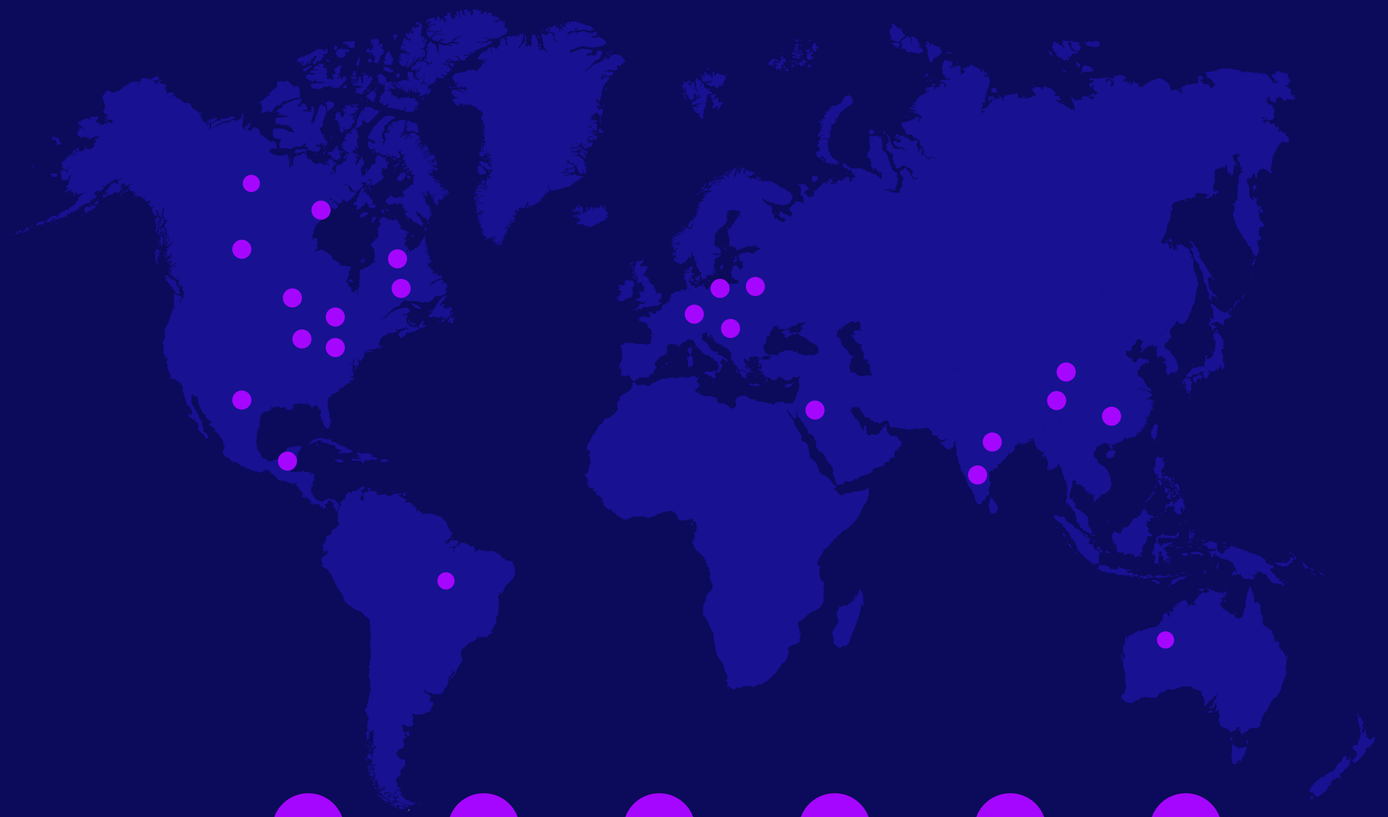


Le nombre de réglementations relatives aux identités numériques a été multiplié par 7 depuis 2010 dans toutes les zones géographiques, tous secteurs d'activité confondus

~25

lois et cadres réglementaires au total se sont concentrés sur des zones géographiques à maturité et des secteurs d'activité particuliers en 2010

Toute | 2010 | 2024



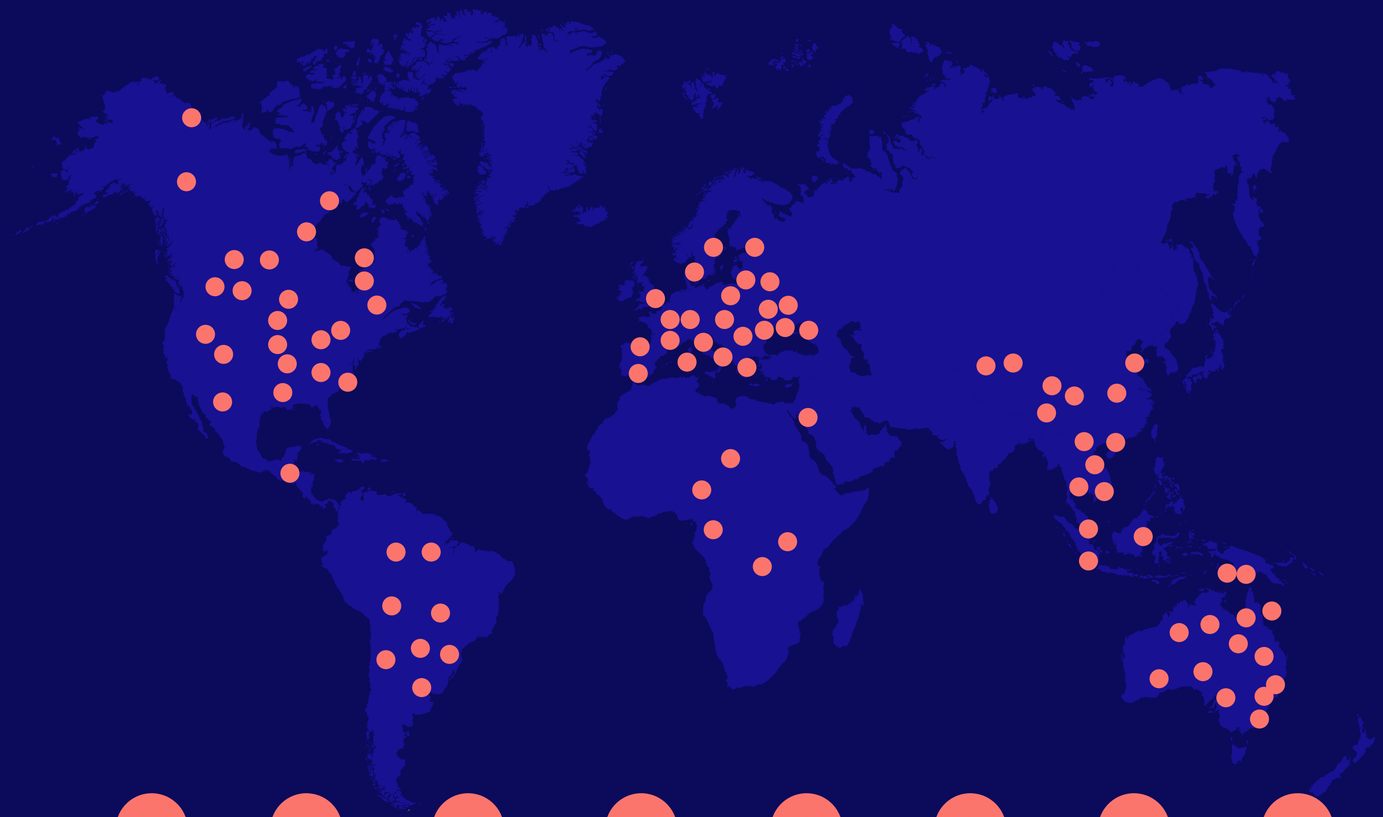
18	2	2	1	1	23
Non corrélées à un secteur	Télécoms	Soins de santé	Secteur financier	Industrie manufacturière	Total

Le nombre de réglementations relatives aux identités numériques a été multiplié par 7 depuis 2010 dans toutes les zones géographiques, tous secteurs d'activité confondus

~135

lois et cadres réglementaires présentant une croissance considérable dans toutes les zones géographiques et dans tous les secteurs d'activité en 2024

Toute | 2010 | 2024



103	11	9	5	3	2	1	134
~6x	~5x	9x	~3x	3x			
Non corrélées à un secteur	Télécoms	Secteur financier	Soin de sante	Industrie manufacturière	Autres	Adminstration	Total

CHAPITRE 4

Comment les entreprises leader de leur secteur s'y prennent pour infléchir la courbe

Commencer le chapitre →

Études de cas
BNP Paribas
Entreprise pharmaceutique
Absa
Currys

Études de cas de quelques entreprises

Partout dans le monde et dans tous les secteurs d'activité, des entreprises de premier plan investissent dans la sécurité des identités numériques pour infléchir la courbe de valeur de la cybersécurité afin d'obtenir des rendements exceptionnels en matière de conformité, d'efficacité opérationnelle, de productivité des utilisateurs et de sécurité.

Objectif :

Réduire les risques cyber et améliorer la productivité

BNP PARIBAS

BNP Paribas Bank Polska a augmenté sa productivité grâce à une automatisation généralisée des tâches IAM autrefois gérées manuellement.

Après une série de fusions, la banque gérait 10 000 utilisateurs et environ 1 000 applications par le biais de programmes IAM décorrélés. Faute d'automatisation, l'équipe informatique n'était pas en mesure de faire face au volume de demandes d'utilisateurs ou de tâches IAM. Après automatisation de ces tâches, toutes les campagnes de certification sont désormais gérées par seulement deux salariés, chacun n'y consacrant que 15 % environ de son temps de travail.

Voir l'étude de cas →

40K

tâches d'identité automatisées exécutées chaque mois

90 %

des demandes d'accès sont exécutées automatiquement

4K

réinitialisations et changements de mot de passe automatisés tous les mois

Objectif :

Améliorer la productivité

Une entreprise pharmaceutique de premier plan comptant 72 000 salariés a amélioré sa productivité et son efficacité en automatisant les tâches IAM.

L'entreprise recherchait un système évolutif hébergé dans le cloud pour remplacer sa solution sur site de gestion des identités, qui était obsolète et nécessitait des interventions manuelles fréquentes. En adoptant un nouveau système hébergé dans le cloud, elle a simplifié la mise en conformité réglementaire et a considérablement réduit le temps consacré aux examens d'accès et le temps d'attente pour obtenir les accès.

40 %

de réduction du temps consacré aux examens d'accès

20 %

de réduction du temps d'attente des accès

30 %

de réduction des tâches manuelles effectuées par les services informatiques

Objectif :

Augmenter la valeur commerciale

Absa, une institution financière panafricaine comptant plus de 35 000 salariés, a simplifié l'intégration et la gestion des identités de son personnel externe, tout en réduisant les coûts.

Afin de se conformer au RGPD Européen et à loi sud-africaine PoPIA, la banque a déployé un outil de gestion des risques basé sur l'IA avec une politique de provisioning « juste-à-temps » et une certification normalisée pour les identités des utilisateurs non-salariés. Ce modèle d'accès basé sur le risque a permis de réduire considérablement les coûts opérationnels et de simplifier la gouvernance des identités pour les sous-traitants et les prestataires externes.

Voir l'étude de cas →

$300
d'économie pour chaque identité intégrée

15
jours économisés pour réaliser l'intégration des identités des tiers

12K
travailleurs non-salariés profitant d'identités sécurisées

Objectif :

Réduction du risque cyber

currys

Currys, un détaillant de produits technologiques basé au Royaume-Uni et comptant plus de 800 magasins, a réduit son profil de risque en améliorant la gouvernance des identités et en automatisant la sécurité des identités.

Currys, un détaillant britannique de produits électroniques comptant plus de 800 magasins outre-Manche, a réduit son profil de risque en améliorant la gouvernance de ses identités numériques et en automatisant leur sécurité. Son ancienne procédure, qui consistait à faire manipuler des tableurs Excel par un personnel en perpétuelle mutation, engendrait un octroi d'accès trop permissifs aux comptes (surprovisioning) ainsi que des risques liés à la conformité. L'automatisation fournit désormais une piste d'audit complète, ce qui réduit les problèmes de conformité et les autorisations non exécutées, tout en renforçant la posture de sécurité globale de l'entreprise.

Voir l'étude de cas →

3x

Currys a divisé les risques cyber par trois en octroyant des privilèges appropriés pour environ 6 000 comptes utilisateurs

210

heures de travail manuel économisées chaque année

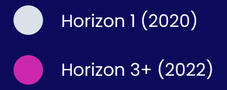
24K

identités gérées

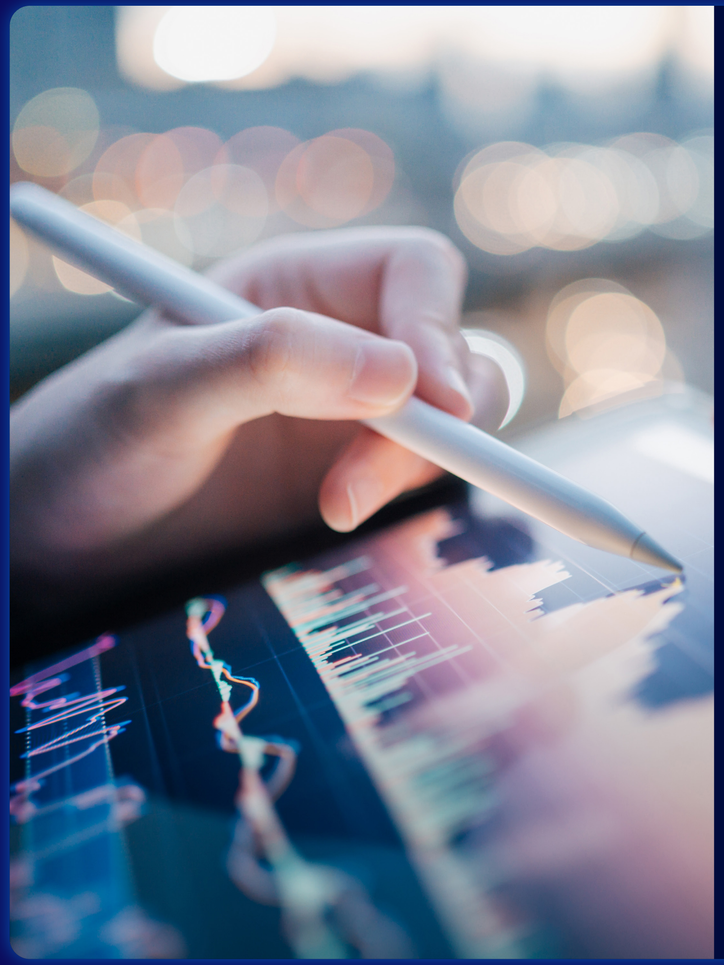
Aboitiz, un conglomérat technologique d'envergure mondiale, est passé directement de l'Horizon 1 à l'Horizon 3 et au-delà en l'espace d'à peine 24 mois, au terme d'un ambitieux projet de « transformation majeure ».

Survolez chaque section pour voir quelle mesure a été adoptée

0 processus formel de gestion des identités et des accès	**21** jours pour la désactivation des comptes utilisateurs et 5 jours pour l'activation	**<5** unités opérationnelles bénéficiant d'une gouvernance centralisée des identités	**<1K** comptes gérés par le biais de processus automatisés
1 programme de gestion unifiée des identités et des accès contrôlant les comptes de l'ensemble du personnel	**0** temps d'attente grâce au provisioning et au deprovisioning instantanés	**47** unités opérationnelles bénéficiant d'une gouvernance centralisée d'environ 23 000 comptes d'application	**144K** modifications et vérifications automatisées des comptes



Voir l'étude de cas →



“

Partis d’une feuille blanche, nous avons effectué un véritable bond en avant en tirant parti des dernières avancées technologiques… Ainsi nous avons pu prendre le temps de la réflexion et consacrer les efforts nécessaires à l’atout le plus précieux de notre entreprise : nos identités numériques.

CISO, Aboitiz Equity Ventures

aboitiz

CHAPTER 5

La voie vers l'horizon suivant

Commencer le chapitre →

La voie vers l'horizon suivant

1. Définir une vision directrice
2. Investir dans les bonnes solutions, notamment celles basées sur l'IA, afin de franchir des horizons et d'obtenir des rendements plus élevés
3. Sécuriser tous les types d'identités
4. Intégrer l'IAM aux opérations de sécurité au sens large afin de permettre une surveillance continue et de garder les primes d'assurance sous contrôle
5. Exploiter les données d'identité pour en tirer des informations exploitables et des politiques de sécurité adaptives
6. Garder une longueur d'avance sur les réglementations et les normes émergentes afin de maintenir la conformité

SailPoint

A quel horizon se situe votre entreprise ?

Pour déterminer votre niveau de maturité en matière de la sécurité des identités :

Faire l'évaluation

Télécharger le rapport complet

IB2567-2501