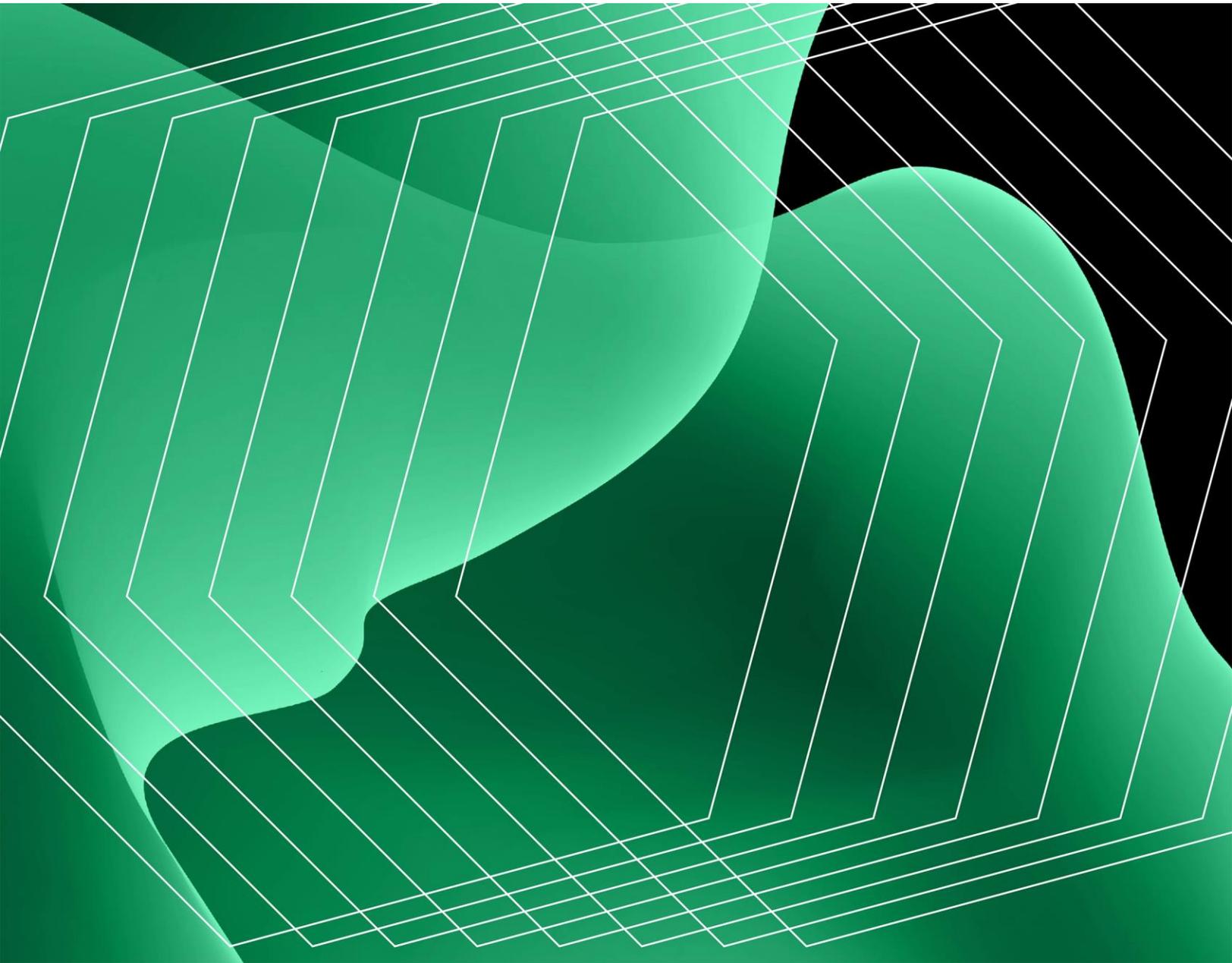


# The Total Economic Impact™ d'Okta Identity Governance

Économies et avantages stratégiques offerts par Identity  
Governance

UNE ÉTUDE TOTAL ECONOMIC IMPACT DE FORRESTER  
COMMANDÉE PAR OKTA, JUIN 2025



## Table des matières

Résumé	3
Le parcours client d'Okta Identity Governance	10
Analyse des bénéfices	14
Analyse des coûts	31
Bilan financier	34

### Consultant :

Kris Peterson

#### À PROPOS DE FORRESTER CONSULTING

Forrester propose des services de conseil indépendants, objectifs et fondés sur la recherche afin d'aider les leaders à obtenir des résultats clés. Sur la base d'études de la clientèle, les équipes de consulting expérimentées de Forrester accompagnent les leaders dans la mise en œuvre de leurs projets stratégiques à l'aide d'un modèle d'engagement unique garantissant un impact durable. Pour en savoir plus, rendez-vous sur [forrester.com/consulting](https://forrester.com/consulting).

© Forrester Research, Inc. Tous droits réservés. Toute reproduction sans autorisation préalable est strictement interdite. Les informations fournies s'appuient sur les meilleures ressources disponibles. Les opinions exprimées reflètent notre jugement à la date de publication du document et sont susceptibles de changer. Forrester®, Technographics®, Forrester Wave et Total Economic Impact sont des marques de Forrester Research, Inc. Toutes les autres marques appartiennent à leurs propriétaires respectifs.

## Résumé

Les entreprises, quelle que soit leur taille, doivent adopter une approche proactive et guidée par des politiques afin de gérer efficacement les accès et les droits. Il s'agit de trouver le juste équilibre entre agilité et évolutivité, d'une part, et contrôle, supervision et conformité, d'autre part, face à l'intensification des menaces de sécurité et à la pression réglementaire croissante, notamment en lien avec la SOX et la PCI-DSS. Des systèmes disparates et des processus manuels créent souvent des angles morts, retardent le provisionnement des accès et contribuent à la surallocation des droits, tout en entraînant des efforts excessifs en matière de reporting. À mesure que les environnements d'identité gagnent en envergure et en complexité, les entreprises ont besoin de solutions de gouvernance qui s'intègrent à l'infrastructure d'identité principale pour soutenir à la fois l'efficacité opérationnelle et la réduction des risques.

[Okta Identity Governance](#) (OIG), une solution de gouvernance et d'administration des identités (IGA) basée sur le cloud, s'intègre directement à l'infrastructure d'identité pour centraliser et automatiser les demandes d'accès, les certifications, les examens des droits, l'application des politiques et la création de rapports. En remplaçant les flux de travail manuels par des automatisations pilotées par événements et une logique d'accès dynamique, Okta Identity Governance (OIG) aide les organisations à appliquer le principe du moindre privilège, à accélérer le provisionnement et le déprovisionnement, et à maintenir la conformité à grande échelle, tout en réduisant la charge administrative et les risques liés aux accès.

Okta a chargé Forrester Consulting de mener une étude Total Economic Impact™ (TEI) afin d'examiner le retour sur investissement (ROI) potentiel que les entreprises peuvent obtenir en déployant Okta Identity Governance.<sup>1</sup> Cette étude a pour objectif de fournir aux lecteurs un cadre de référence qui leur permet d'évaluer l'impact financier potentiel de l'utilisation d'Okta Identity Governance dans leur entreprise.



Retour sur investissement (ROI)

**211 %**



Valeur actuelle nette

**1,8 M\$**

Pour mieux cerner les bénéfices, les coûts et les risques de cet investissement, Forrester a interrogé huit décideurs qui utilisent OIG. Pour les besoins de cette étude, Forrester a regroupé

## RESUME

les expériences des personnes interrogées et a combiné les résultats en une seule [entreprise de référence](#), qui est une entreprise mondiale avec un chiffre d'affaires annuel de 1,5 milliard de dollars, 5 000 identités, 100 applications et 12 employés responsables de la gestion des identités et des accès (IAM), de l'aide à l'audit et de l'application des règles de conformité.

Les personnes interrogées ont déclaré qu'avant de déployer OIG, leurs environnements dépendaient fortement du travail manuel, d'outils fragmentés et de politiques d'accès incohérentes, ce qui entraînait des inefficacités, des erreurs humaines et des vulnérabilités en termes de sécurité. Les tentatives précédentes de formalisation de la gouvernance des identités se sont souvent révélées incomplètes ou non viables, entraînant des retards de provisionnement, une surallocation des droits, des frictions lors des audits et une exposition accrue aux risques.

Après l'investissement dans OIG, les personnes interrogées ont fait état d'un passage d'un contrôle réactif à une gouvernance proactive, guidée par des politiques. Les équipes chargées de l'IAM ont bénéficié d'une visibilité centralisée, ont automatisé les flux de travail essentiels et ont appliqué les contrôles d'accès de manière plus cohérente, ce qui a permis d'accélérer la prestation de services, de simplifier les audits et de renforcer la posture de sécurité.

## PRINCIPALES CONCLUSIONS

**Bénéfices quantifiés.** Pour l'entreprise de référence, les bénéfices quantifiés en valeur actuelle (VA) ajustée en fonction des risques sur une période de trois ans sont les suivants :

- **Amélioration de l'efficacité de la gouvernance des identités pour un montant de 1,1 million de dollars.** L'automatisation des demandes d'accès, des examens de certification et de la gestion des droits réduit jusqu'à 60 % les efforts requis par les équipes chargées de l'IAM et du support informatique de l'entreprise. Ces économies reflètent la réduction du travail manuel lié aux examens d'accès, à la gestion des droits et aux demandes d'accès ponctuelles, ainsi que le temps gagné par les responsables lors des cycles d'examen et d'approbation des accès.
- **Réduction des efforts de préparation des audits et des rapports de conformité, pour un total de 232 000 \$.** L'amélioration de la visibilité des accès et l'automatisation des examens simplifient la collecte de preuves et réduisent le temps nécessaire à l'entreprise pour répondre aux demandes d'audit interne et externe, notamment celles liées à la SOX, la PCI-DSS et autres cadres réglementaires. L'entreprise de référence bénéficie également d'une meilleure cohérence dans les flux de travail de certification et

de contrôle des accès, ce qui permet d'éviter les constats d'audit et de renforcer sa posture globale de gouvernance.

- **Amélioration de l'efficacité de la plateforme et rationalisation des logiciels, entraînant des gains d'efficacité de 567 000 \$.** En remplaçant les outils existants et les connecteurs coûteux par des intégrations prêtes à l'emploi et en améliorant la visibilité des droits, l'entreprise de référence évite les coûts de licence et de conseil tout en réduisant les efforts administratifs liés à l'intégration, à la désinscription et aux changements d'accès. Les flux de travail de gouvernance automatisent les processus clés d'intégration, de transfert et de départ, tout en permettant une application des politiques sans augmentation des effectifs.
- **Accroissement de la productivité grâce à l'amélioration de la gouvernance des accès évalué à 497 000 \$.** Les utilisateurs finaux, les responsables et les propriétaires d'applications composites consacrent moins de temps à naviguer dans les chaînes d'approbation manuelles ou à résoudre des problèmes d'accès, et plus de temps à d'autres tâches à valeur ajoutée pour l'entreprise. Un gain de temps par utilisateur, même modeste, peut faire la différence lorsqu'il est appliqué à une large base d'utilisateurs. Des expériences utilisateur rationalisées et des flux de travail cohérents et adaptés aux audits réduisent les retards et augmentent la flexibilité de l'entreprise.
- **Réduction du risque de violation de la sécurité, d'une valeur estimée à 231 000 \$.** L'entreprise de référence réduit son exposition mesurable aux failles de sécurité en renforçant sa posture de gouvernance et en éliminant les accès excessifs ou obsolètes. L'automatisation de la gouvernance et les examens proactifs des droits limitent le risque d'abus de privilèges et de menaces internes tout en permettant une empreinte plus cohérente de la politique d'accès à travers les systèmes.

**Bénéfices non quantifiés.** Les bénéfices qui apportent de la valeur à l'entreprise de référence, mais qui ne sont pas quantifiés dans cette étude, sont les suivants :

- **Rentabilisation plus rapide.** Okta Identity Governance se déploie rapidement par rapport aux solutions IGA traditionnelles. L'entreprise de référence constate une valeur d'automatisation immédiate, une intégration plus rapide des utilisateurs et des applications, ainsi qu'une période de montée en puissance notablement courte, accélérant la réalisation des avantages quantifiés de quelques semaines ou mois.
- **Renforcement de la satisfaction de l'équipe chargée de l'IAM.** Les équipes de l'entreprise de référence passent de tâches manuelles et répétitives de gouvernance des

identités à des activités stratégiques à plus forte valeur ajoutée, telles que la conception de politiques, la gestion des exceptions et la planification de la feuille de route.

- **Amélioration de l'expérience des employés et des utilisateurs finaux.** Les utilisateurs finaux subissent moins de retards ou d'interruptions d'accès, et les responsables passent moins de temps à examiner ou à approuver les certifications et les demandes d'accès. En permettant un accès en libre-service et des processus d'approbation simplifiés, l'entreprise de référence réduit les frictions et améliore l'accès aux systèmes critiques de l'entreprise.

**Coûts.** Pour l'entreprise de référence, les coûts sur trois ans en VA ajustée en fonction des risques sont les suivants :

- **Frais de licence d'OIG : 821 000 \$.** Ce montant reflète le coût total des licences pour les fonctionnalités d'OIG et l'assistance standard pour une base d'utilisateurs de 5 000 identités.
- **Les efforts de mise en œuvre et de déploiement s'élèvent à 28 000 \$.** Ce montant comprend l'installation ponctuelle, la gestion interne du projet et le travail de configuration, ainsi qu'un léger effort continu pour maintenir les flux de travail et les politiques de gouvernance.

L'analyse financière, fondée sur les entretiens, a révélé que l'entreprise de référence réalisait des bénéfices d'un montant de 2,6 millions de dollars sur trois ans pour des coûts de 849 000 \$, soit une valeur actuelle nette (VAN) de 1,8 million de dollars et un ROI de 211 %.

Économies totales de main-d'œuvre et gains d'efficacité dans les efforts de gouvernance des identités, d'audit et de conformité, ainsi que dans les améliorations de la gouvernance des accès

**1,8 M\$**

« [OIG] fait tout ce qu'il est censé faire dès le premier jour, et même plus. Vous bénéficiez des capacités dont vous avez besoin pour être en conformité, et vos utilisateurs sont satisfaits. Cela résume parfaitement cet outil. »

DIRECTEUR PRINCIPAL, RESPONSABLE MONDIAL DE L'IAM, SERVICES PROFESSIONNELS

« Si l'on considère les économies de main-d'œuvre pour tous les utilisateurs, qu'il s'agisse du service desk, de la sécurité, de l'audit, des propriétaires d'applications et des responsables d'entreprise qui doivent examiner et approuver les demandes d'accès, les économies de main-d'œuvre justifient le coût global. Ensuite, la réduction des risques pour l'entreprise et la façon dont cela améliore notre posture de sécurité en général constituent également un énorme avantage. »

DSI, SERVICES FINANCIERS

## RESUME



ROI

**211 %**



BÉNÉFICES EN VA

**2,6 M\$**



VALEUR ACTUELLE  
NETTE (VAN)

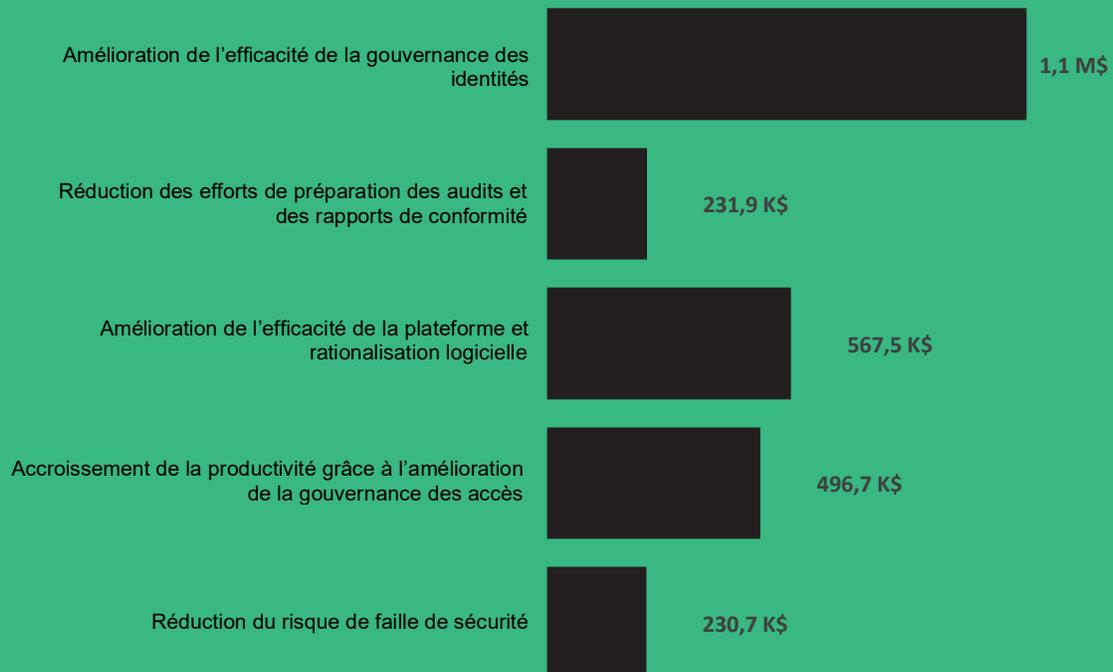
**1,8 M\$**



DÉLAI DE  
RÉCUPÉRATION

**< 6 mois**

### Bénéfices (sur trois ans)



## CADRE DE RÉFÉRENCE ET MÉTHODOLOGIE TEI

À partir des informations collectées lors de ces entretiens, Forrester a créé un cadre de référence Total Economic Impact™ pour les entreprises qui envisagent d'investir dans Identity Governance.

L'objectif de ce cadre de référence est d'identifier les différents facteurs (coûts, bénéfices, flexibilité et risques) qui influencent la décision d'investissement. Forrester a utilisé une approche en plusieurs étapes pour évaluer l'impact qu'Identity Governance peut avoir sur une entreprise.

### AVERTISSEMENTS

Remarques à l'intention des lecteurs et des lectrices :

L'étude est commandée par Okta et réalisée par Forrester Consulting. Elle n'est pas destinée à être utilisée en tant qu'analyse concurrentielle.

Forrester n'émet aucune hypothèse concernant le retour sur investissement (ROI) que d'autres entreprises pourraient obtenir. Forrester recommande vivement aux lecteurs d'utiliser leurs propres estimations dans les limites du cadre de référence fourni dans l'étude pour déterminer la pertinence d'investir dans Identity Governance.

Identity Governance a relu l'étude et fourni des commentaires à Forrester, mais Forrester garde le contrôle éditorial de l'étude et de ses conclusions et n'accepte pas de modifications de l'étude qui contrediraient ses conclusions ou occulteraient le propos de l'étude.

Okta a fourni les noms des clients pour les entretiens, mais n'a pas pris part à ces derniers.

### 1. Diligence raisonnable

Nous nous sommes entretenus avec les parties prenantes d'Okta et les analystes de Forrester pour recueillir des données relatives à Identity Governance.

### 2. Entretiens

Nous nous sommes entretenus avec huit représentants d'entreprises qui utilisent Identity Governance pour obtenir des données concernant les coûts, les bénéfices et les risques.

### 3. Entreprise de référence

Nous avons défini une entreprise de référence d'après les caractéristiques des entreprises des personnes interrogées.

### 4. Cadre du modèle financier

Nous avons élaboré un modèle financier à partir des entretiens menés, en utilisant la méthodologie TEI, puis en ajustant ce modèle en fonction des risques sur la base des interrogations et des préoccupations des personnes interrogées.

### 5. Étude de cas

Nous avons utilisé quatre éléments fondamentaux du TEI pour modéliser l'impact de l'investissement : bénéfices, coûts, flexibilité et risques. Compte tenu de la sophistication croissante des analyses ROI associées aux investissements dans le secteur informatique, la méthodologie TEI de Forrester offre une vue d'ensemble exhaustive de l'impact économique total des décisions d'achat. Pour en savoir plus sur la méthodologie TEI, veuillez vous reporter à l'Annexe A.

# Le parcours client d'Okta Identity Governance

## Facteurs qui déterminent l'investissement dans Identity Governance

Entretiens			
Fonction	Secteur d'activité	Région	Identités/applications gérées
Directeur, IAM	Services informatiques	Siège en Amérique du Nord, présence mondiale	104 000/200
Directeur de l'architecture de sécurité	Conseil en informatique	Siège en Amérique du Nord, présence mondiale	100 000/1 500
Directeur général	Services financiers	Siège en Amérique du Nord, présence mondiale	70 000/90
Directeur principal, responsable mondial de l'IAM	Services professionnels	Siège en Amérique du Nord, présence mondiale	8 000/400
DSI	Services financiers	Siège dans la zone EMEA, présence mondiale	8 000/100
Directeur de la sécurité de l'information	Santé	Amérique du Nord	7 200/370
Architecte de solutions informatiques	Logiciels	Siège en Amérique du Nord, présence mondiale	3 000/70
RSSI	Services informatiques	EMEA	2 200/200

## PRINCIPAUX DÉFIS

Avant de déployer Okta Identity Governance, les personnes interrogées ont évoqué des environnements d'identité fragmentés, façonnés par un mélange de plateformes IGA héritées, d'outils maison et de processus manuels. Ces environnements étaient source d'inefficacité opérationnelle pour les équipes informatiques et de lacunes en termes de conformité et de contrôle d'accès pour les équipes de sécurité. Les demandes d'accès étaient souvent basées sur des tickets, les certifications reposaient sur des feuilles de calcul et la gestion des droits manquait de standardisation. Ces limitations ont engendré des expériences incohérentes pour les utilisateurs et augmenté les risques de non-conformité ; elles ont également imposé une charge de travail excessive au personnel informatique et de sécurité.

Les personnes interrogées ont mis en évidence plusieurs défis communs, notamment :

- **Un provisionnement manuel et des changements d'accès qui retardent la productivité et créent des risques.** De nombreuses personnes interrogées ont fait remarquer que l'accès était accordé ou révoqué via des tickets du service d'assistance avec des objectifs SLA de cinq jours ou plus ; d'autres ont ajouté que les utilisateurs conservaient souvent un accès inapproprié longtemps après avoir changé de rôle ou avoir quitté l'entreprise, ce qui augmentait le risque d'escalade de privilèges ou de menace interne. L'architecte de solutions informatiques a expliqué que les demandes d'accès submergeaient son équipe et qu'il avait dû mobiliser d'autres collaborateurs pour l'aider : « Nous étions une trentaine de personnes impliquées. Les demandes ont été réparties de manière égale entre tous parce qu'il était impossible que ma petite équipe de trois personnes chargées de la gestion des accès puisse traiter toutes les demandes d'accès qui nous parvenaient, si bien que c'est devenu un effort conjoint. »
- **Des certifications d'accès lentes, laborieuses et sujettes aux erreurs.** Les entreprises s'appuyaient en grande partie sur des feuilles de calcul et des attestations manuelles pour répondre aux exigences d'audit et de conformité. Plusieurs personnes interrogées ont signalé que les certifications exigeaient souvent des semaines de préparation par le personnel de l'IAM et des heures de révision par les responsables et les propriétaires d'entreprise. Le directeur de la sécurité de l'information dans le secteur des soins de santé a qualifié les campagnes « d'expérience pénible » et a déclaré : « Nous n'achevons jamais réellement nos certifications. Elles échouaient au beau milieu de la campagne en raison de la réticence des dirigeants. Ils refusaient de les effectuer, si bien que nous ne pouvions jamais dire que nous avons réellement respecté notre politique. »
- **Une gestion des droits qui manque de visibilité et de normalisation.** En l'absence d'une gouvernance centralisée, l'accès basé sur les rôles était appliqué de manière incohérente et les utilisateurs accumulaient fréquemment des droits excessifs ou obsolètes. Le directeur principal, responsable mondial de l'IAM dans les services professionnels, a expliqué que « les employés accumulaient souvent les accès » et que son équipe devait signaler et résoudre manuellement les comptes surprovisionnés.
- **Une préparation à l'audit qui demande beaucoup de temps et de coordination.** Les personnes interrogées ont qualifié les audits de très perturbants pour OIG, nécessitant souvent des semaines de préparation et plusieurs membres du personnel pour compiler les journaux d'accès, suivre les examens et répondre aux conclusions de l'audit.

« Tout le monde redoutait notre intervention [avant OIG], et maintenant nous sommes considérés comme un facilitateur d'activité. C'est vraiment très fort. »

ARCHITECTE DE SOLUTIONS INFORMATIQUES, LOGICIELS

« Nous avons supprimé un grand nombre de tâches manuelles qui étaient sujettes à des erreurs et augmenté la précision de notre gestion des comptes et du provisionnement [avec OIG], qu'il s'agisse d'applications, d'utilisateurs ou de clients. »

DSI, SERVICES FINANCIERS

## ENTREPRISE DE RÉFÉRENCE

À partir des entretiens, Forrester a défini un cadre de référence TEI, une entreprise de référence ainsi qu'une analyse du ROI qui illustre les domaines affectés financièrement. L'entreprise de référence est représentative des entreprises interrogées par Forrester. Elle est utilisée pour présenter l'analyse financière sous forme agrégée dans la section suivante. Voici ses principales caractéristiques :

**Description de l'entreprise de référence.** Cette entreprise internationale génère un chiffre d'affaires annuel de 1,5 milliard de dollars et compte 5 000 identités et 100 applications. L'équipe chargée de l'IAM comprend 10 ETP couvrant l'ingénierie des identités, les opérations de gouvernance, l'application des politiques et les campagnes de certification, ainsi que deux ETP fournissant un soutien en matière d'audit et de conformité. Avant l'intégration avec OIG, l'entreprise utilise Okta pour les services d'identité de base en parallèle d'une solution héritée distincte et de processus manuels pour la gouvernance des accès.

**Caractéristiques du déploiement.** L'entreprise de référence déploie les composants d'OIG pour la certification et les demandes d'accès, la gestion des droits, les rapports d'audit et de conformité, et l'automatisation via Okta Workflows au cours d'une période de mise en œuvre de huit semaines au début de l'Année 1.

#### **HYPOTHÈSES PRINCIPALES**

1,5 milliard de dollars de chiffre d'affaires

5 000 identités

Une équipe chargée de l'IAM composée de 10 ETP gérant la gouvernance des identités et deux ETP fournissant un support pour l'audit et la conformité.

# Analyse des bénéfices

Données relatives aux bénéfices quantifiés appliquées à l'entreprise de référence

Total des bénéfices						
Réf.	Bénéfice	Année 1	Année 2	Année 3	Total	Valeur actuelle
Atr	Amélioration de l'efficacité de la gouvernance des identités	323 366 \$	475 538 \$	570 645 \$	1 369 548 \$	1 115 709 \$
Btr	Réduction des efforts de préparation des audits et des rapports de conformité	69 401 \$	99 144 \$	115 668 \$	284 213 \$	231 932 \$
Ctr	Amélioration de l'efficacité de la plateforme et rationalisation logicielle	225 900 \$	229 500 \$	229 500 \$	684 900 \$	567 460 \$
Dtr	Accroissement de la productivité grâce à l'amélioration de la gouvernance des accès	199 750 \$	199 750 \$	199 750 \$	599 250 \$	496 749 \$
Etr	Réduction du risque de faille de sécurité	92 757 \$	92 757 \$	92 757 \$	278 270 \$	230 672 \$
	Total des bénéfices (valeurs ajustées en fonction des risques)	911 173 \$	1 096 688 \$	1 208 320 \$	3 216 181 \$	2 642 522 \$

## AMÉLIORATION DE L'EFFICACITÉ DE LA GOUVERNANCE DES IDENTITÉS

**Éléments probants et données.** Les personnes interrogées ont fait état de processus manuels étendus pour les certifications d'accès, la gestion des droits et le traitement des demandes d'accès ponctuelles avant le déploiement d'Okta Identity Governance.

- Le directeur de l'IAM d'une entreprise de services informatiques a évoqué la place importante qu'accordait son équipe aux automatisations et aux capacités de libre-service. Il a expliqué que : « Le volume [de travail IAM qui] occupait plus de 36 [personnes] à temps plein alors qu'aujourd'hui, nous réalisons l'essentiel avec seulement cinq [personnes via OIG]. ... Grâce à leurs capacités et à l'automatisation de Workflows, nous ne développons plus ni ne construisons d'infrastructures pour ces tâches. Nous opérons directement sur la plateforme Okta en utilisant leurs Workflows à faible code/sans code pour automatiser les processus.

## ANALYSE DES BÉNÉFICES

- Le directeur de l'IAM a ajouté que l'entreprise mène entre 80 et 90 campagnes par mois, couvrant 20 000 à 80 000 éléments, chacune nécessitant moins d'une heure de travail à l'équipe chargée de l'IAM.
- Le directeur de la sécurité de l'information d'une entreprise de soins de santé a confié : « Du côté de l'infosec, il fallait environ quatre semaines à un ingénieur et à un analyste pour préparer une campagne. Ils devaient ensuite s'en occuper et assister les responsables, parfois plusieurs centaines à la fois. Deux ressources étaient pratiquement immobilisées pendant un quart de l'année pour effectuer des vérifications d'accès. ... La mise en place d'une telle campagne prend désormais 30 minutes ».
- Le DSI d'une société de services financiers a déclaré : « Nous sommes passés d'une automatisation de 50 % à 90 % [avec OIG] [avec une] réduction de 50 % de la main d'œuvre. »
- Le directeur principal, responsable mondial de l'IAM dans une entreprise de services professionnels a estimé que son équipe chargée de l'IAM composée de neuf personnes fait maintenant le travail de 14 à 15 personnes.
- Le RSSI des services informatiques a mentionné l'automatisation fournie par OIG comme l'un des principaux avantages, expliquant que l'entreprise a « fondamentalement tout construit sur des flux de travail et des processus automatisés pour supprimer cet effort manuel ».
- L'architecte de solutions informatiques d'une entreprise de logiciels a évoqué l'impact des Workflows Okta : « Nous disposions d'une automatisation, mais c'était un amalgame de tout, à savoir des scripts PowerShell, des scripts Python, des fonctions AWS Lambda, un peu partout. Nous avons pu migrer tout cela dans la pile Okta Workflow, puis utiliser les crochets intégrés dans toutes nos différentes opérations liées à l'identité, ce qui a considérablement réduit la complexité et aussi le temps nécessaire pour maintenir ces différentes plateformes ».

**Modélisation et hypothèses.** Compte tenu des informations recueillies lors des entretiens, Forrester émet les hypothèses suivantes concernant l'entreprise de référence :

- Dix ETP IAM sont affectés aux tâches essentielles de gouvernance des identités, telles que les demandes et examens d'accès et la gestion des droits.
- Le salaire annuel moyen, toutes charges comprises, d'un ETP IAM est de 140 900 \$.

## ANALYSE DES BÉNÉFICES

- Après la période de déploiement de huit semaines, l'équipe économise 40 % du temps consacré aux tâches de gouvernance des identités pendant les 44 semaines restantes, soit une économie nette de 34 % au cours de l'Année 1.
- Le gain de temps passe à 50 % au cours de l'Année 2 et à 60 % au cours de l'Année 3, car OIG gère davantage d'applications et intègre davantage d'automatismes, ce qui réduit encore les efforts manuels préalables.
- Ces gains de temps sont réaffectés à d'autres activités à valeur ajoutée à hauteur de 75 %.

**Risques.** Pour garantir des estimations réalistes et défendables, Forrester applique des ajustements de risque basés sur la cohérence des entretiens et le degré de variation des résultats rapportés. Cette composante de la méthodologie TEI permet de tenir compte des différences qui existent entre les environnements déployés. Le montant de ce bénéfice peut varier d'un client à l'autre en raison des différences suivantes :

- Le niveau d'automatisation et de gain de temps, qui peut varier en fonction de la complexité du système existant ou des exigences de conformité.
- Le besoin de supervision manuelle, qui peut être plus important dans les entreprises soumises à des contraintes réglementaires ou sectorielles.
- L'ampleur du bénéfice, qui dépend du volume d'utilisateurs, de la fréquence des campagnes, ainsi que du nombre et de la complexité des applications régies.
- Le salaire annuel moyen d'un ETP IAM.

**Résultats.** Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 10 % et a ainsi obtenu une valeur actuelle (VA) totale ajustée en fonction des risques (taux d'actualisation de 10 %) de 1,1 million de dollars sur trois ans.

Temps gagné sur les tâches de gouvernance des identités à l'Année 3

**60 %**

« Nous effectuons facilement près de dix fois plus de travail qu'à l'époque où nous utilisions uniquement [l'ancienne solution], et peut-être même encore plus. »

DIRECTEUR DE LA SÉCURITÉ DE L'INFORMATION, SECTEUR DE LA SANTÉ

« Les flux de travail permettent d'économiser beaucoup d'ETP. Compte tenu du nombre d'applications que nous possédons, il serait autrement presque impossible de les gérer. »

DIRECTEUR DE L'ARCHITECTURE DE SÉCURITÉ, CONSEIL EN INFORMATIQUE

### Amélioration de l'efficacité de la gouvernance des identités

Réf.	Indicateur	Source	Année 1	Année 2	Année 3
A1	ETP IAM affectés aux demandes et examens d'accès, à la gestion des droits et à d'autres tâches de gouvernance des identités	Entreprise de référence	10	10	10
A2	Salaire annuel toutes charges comprises d'un ETP IAM chargé de tâches de gouvernance des identités	Entreprise de référence	140 900 \$	140 900 \$	140 900 \$
A3	Temps net gagné après avoir déployé OIG pour les tâches de gouvernance des identités	Entretiens	34 %	50 %	60 %
A4	Productivité récupérée	Méthodologie TEI	75 %	75 %	75 %
At	Amélioration de l'efficacité de la gouvernance des identités	$A1 * A2 * A3 * A4$	359 295,0 \$	528 375,0 \$	634 050,0 \$
	Ajustement en fonction des risques	↓ 10 %			
Atr	Amélioration de l'efficacité de la gouvernance des identités (valeur ajustée en fonction des risques)		323 365,50 \$	475 537,50 \$	570 645,00 \$
<b>Total sur trois ans : 1 369 548 \$</b>			<b>Valeur actuelle sur trois ans : 1 115 709 \$</b>		

## RÉDUCTION DES EFFORTS DE PRÉPARATION DES AUDITS ET DES RAPPORTS DE CONFORMITÉ

**Éléments probants et données.** Les personnes interrogées ont déclaré qu'OIG aide à rationaliser ou à éviter les efforts manuels importants liés aux audits récurrents, aux examens d'accès et aux rapports de conformité. Les équipes précédemment chargées de valider les contrôles d'accès et de préparer les preuves et les rapports ont fait état de gains de temps importants et d'une réduction des efforts liés aux audits. Les domaines spécifiques dans lesquels les efforts ont été réduits ou évités sont les suivants.

- Les personnes interrogées ont décrit les semaines de préparation d'audit nécessaires avant OIG, qui impliquaient la collecte manuelle de données de certification, la réalisation de captures d'écran des approbations d'accès et la validation des journaux de contrôle d'accès dans les différents systèmes.
- Plusieurs personnes interrogées ont observé que les flux de travail automatisés de certification amélioreraient l'exhaustivité et la cohérence des processus d'examen, réduisant ainsi le risque d'omissions ou d'erreurs pouvant entraîner des constats d'audit. Elles ont également indiqué que la centralisation des politiques, des flux de travail et des journaux d'audit au sein d'OIG contribuait à réduire les efforts nécessaires pour expliquer les processus de gouvernance aux auditeurs et pour documenter les exceptions.
- Les personnes interrogées ont décrit le gain de temps et la réduction de la complexité en utilisant les tableaux de bord d'OIG pour générer des rapports ad hoc sur les examens d'accès, les rôles des utilisateurs et les droits. Ces fonctionnalités ont aidé les équipes à répondre plus rapidement aux demandes d'audit interne ou de réglementation externe.
- Le directeur principal, responsable mondial de l'IAM dans les services professionnels, a expliqué que sans l'automatisation d'OIG, une équipe de trois à cinq personnes aurait été nécessaire pour gérer la cohérence de la collecte d'éléments de preuve.
- Le directeur principal a ajouté :« Je peux faire une présentation à un auditeur en une seule session de 30 minutes et en avoir terminé. Aucun suivi. (...) [L'auditeur] est revenu vers moi en demandant à son ingénieur en sécurité de prendre contact avec [nous] afin de déployer [OIG]. Cela s'est produit deux fois. ... C'est le plus beau compliment qui soit. ».

**Modélisation et hypothèses.** Compte tenu des informations recueillies lors des entretiens, Forrester émet les hypothèses suivantes concernant l'entreprise de référence :

- Les tâches d'audit et de conformité sont confiées à deux ETP.
- Le salaire annuel moyen, toutes charges comprises, d'un ETP IAM est de 122 400 \$.
- Après la période de déploiement de huit semaines, l'équipe économise 50 % du temps consacré à la préparation de l'audit et aux tâches de reporting de conformité pendant les 44 semaines restantes, soit une économie nette de 42 % au cours de l'Année 1.
- Le gain de temps passe à 60 % à l'Année 2 et à 70 % à l'Année 3, à mesure que l'équipe chargée de l'IAM gagne en efficacité et que la gouvernance d'OIG s'étend.
- Ces gains de temps sont réaffectés à d'autres activités à valeur ajoutée à hauteur de 75 %.

**Risques.** Le montant de ce bénéfice peut varier d'un client à l'autre en raison des différences suivantes :

- Le nombre et la complexité des audits requis en fonction du secteur d'activité et de la zone géographique.
- La maturité des processus et outils existants avant l'adoption d'OIG.
- La taille et la structure des équipes chargées de l'IAM et de la conformité.
- Le degré d'automatisation des tâches liées à l'audit ou leur intégration dans d'autres systèmes de gouvernance.
- Le salaire annuel moyen, toutes charges comprises, d'un ETP IAM.

**Résultats.** Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 10 %, et a ainsi obtenu une valeur actuelle (VA) totale ajustée en fonction des risques (taux d'actualisation de 10 %) de 232 000 \$ sur trois ans.

Gain de temps sur les tâches d'audit et de conformité à l'Année 3

**70 %**

Réduction des efforts de préparation des audits et des rapports de conformité					
Réf.	Indicateur	Source	Année 1	Année 2	Année 3
B1	ETP IAM avec tâches d'audit et de conformité	Entreprise de référence	2	2	2
B2	Salaire annuel toutes charges comprises d'un ETP IAM chargé de tâches d'audit et de conformité	Entreprise de référence	122 400 \$	122 400 \$	122 400 \$
B3	Gain de temps net sur les tâches d'audit et de conformité avec OIG	Entretiens	42 %	60 %	70 %
B4	Productivité récupérée	Méthodologie TEI	75 %	75 %	75 %
Bt	Réduction des efforts de préparation des audits et des rapports de conformité	B1*B2*B3*B4	77 112,00 \$	110 160,00 \$	128 520,00 \$
	Ajustement en fonction des risques	↓ 10 %			
Btr	Réduction des efforts de préparation des audits et des rapports de conformité (valeur ajustée en fonction des risques)		69 400,80 \$	99 144,00 \$	115 668,00 \$
<b>Total sur trois ans : 284 213 \$</b>			<b>Valeur actuelle sur trois ans : 231 932 \$</b>		

## AMÉLIORATION DE L'EFFICACITÉ DE LA PLATEFORME ET RATIONALISATION LOGICIELLE

**Éléments probants et données.** Les personnes interrogées ont déclaré qu'Okta Identity Governance avait amélioré l'efficacité de la plateforme en réduisant le recours à des consultants externes coûteux, en éliminant les connecteurs personnalisés et en donnant aux équipes internes les moyens d'utiliser des outils à faible codage ou sans codage. Parallèlement, les entreprises ont acquis une meilleure visibilité sur les droits et des perspectives d'utilisation, ce qui leur a permis de rationaliser les dépenses logicielles et de supprimer les licences inutilisées. Dans leur ensemble, ces évolutions ont accru l'efficacité opérationnelle et consolidé la portée de la gouvernance.

Efficacité de la plateforme :

- Le directeur de la sécurité de l'information dans le secteur de la santé a déclaré qu'avant OIG, son entreprise dépensait 150 000 à 200 000 \$ par an en consultants pour faire progresser les initiatives de solutions héritées. Avec OIG, ce coût supplémentaire n'est plus nécessaire grâce aux connecteurs prêts à l'emploi, aux automatisations à faible codage ou sans codage et aux ressources internes habilitées par des outils plus modernes.

## ANALYSE DES BÉNÉFICES

- Le DSI du secteur des services financiers ajoute : « [OIG] est livré avec un grand nombre d'intégrations prédéfinies, ce qui a facilité la connexion à notre environnement actuel. ... [OIG nous aide également] à tirer profit de la gestion des licences et des ressources en réduisant le nombre de comptes inutilisés ».
- Le directeur principal, responsable mondial de l'IAM, a fait remarquer que sa société de services professionnels payait entre 15 000 et 25 000 \$ pour connecter des applications et qu'en conséquence : « Vous ne connectez pas tous les systèmes que vous auriez dû connecter [pour] la gouvernance, et vous risquez donc d'avoir des lacunes parce qu'ils ne sont pas connectés via une API... [Avec OIG], tout ce qui était connecté par SSO à mon fournisseur d'identité était automatiquement ajouté à la gouvernance, comme il se doit ».

### Rationalisation logicielle :

- Les personnes interrogées ont expliqué que la visibilité offerte par OIG sur les droits d'accès avait permis d'identifier et de supprimer les licences inutilisées ou en double. L'architecte de solutions informatiques a déclaré que sa société de logiciels menait des campagnes de certification ponctuelles afin d'obtenir une visibilité en temps réel sur les utilisateurs effectifs des applications, et qu'elle avait « constaté un avantage considérable à chaque déploiement ». Un exemple a permis de réduire d'environ 200 le nombre de licences pour une application comptant 550 utilisateurs, pour un coût de 5 à 10 \$ par utilisateur et par mois.
- Interrogé sur les économies liées à l'efficacité des plateformes et à la rationalisation des logiciels, le DSI d'une société de services financiers a estimé que son entreprise économisait plus de 200 000 dollars par an.

**Modélisation et hypothèses.** Compte tenu des informations recueillies lors des entretiens, Forrester émet les hypothèses suivantes concernant l'entreprise de référence :

- L'entreprise connecte 10 applications supplémentaires à l'aide d'OIG qui auraient nécessité un connecteur payant dans le cadre de l'ancienne solution.
- Les frais de connexion s'élèvent à 20 000 \$ par application.
- OIG permet de supprimer les licences pour 10 applications, avec une moyenne de 50 licences inutilisées ou en double supprimées et un coût mensuel de 5 \$ par licence.
- Après la période de déploiement de huit semaines, l'entreprise économise 21 000 \$ en services de conseil ou en assistance tierce au cours de l'Année 1 et 25 000 \$ au cours des Années 2 et 3.

## ANALYSE DES BÉNÉFICES

**Risques.** Le montant de ce bénéfice peut varier d'un client à l'autre en raison des différences suivantes :

- Le coût et la disponibilité des connecteurs préconstruits pour les solutions IGA existantes.
- Le nombre et les types d'applications ajoutées ou régies via OIG.
- Les structures de licence et les modèles de surprovisionnement dans les environnements logiciels de l'entreprise.
- Le recours à des consultants externes ou à des fournisseurs de services gérés pour les fonctions IAM.

**Résultats.** Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 10 %, et a ainsi obtenu une valeur actuelle (VA) totale ajustée en fonction des risques (taux d'actualisation de 10 %) de 568 000 \$ sur trois ans.

<b>Amélioration de l'efficacité de la plateforme et rationalisation logicielle</b>					
<b>Réf.</b>	<b>Indicateur</b>	<b>Source</b>	<b>Année 1</b>	<b>Année 2</b>	<b>Année 3</b>
C1	Frais de connexion à l'ancienne solution par application	Entretiens	20 000 \$	20 000 \$	20 000 \$
C2	Connexions d'applications supplémentaires possibles grâce à OIG	Entreprise de référence	10	10	10
<b>C3</b>	<b>Sous-total : frais de connexion évités grâce à OIG</b>	<b>C1*C2</b>	<b>200 000 \$</b>	<b>200 000 \$</b>	<b>200 000 \$</b>
C4	Applications dont les licences ont été éliminées grâce à OIG	Entreprise de référence	10	10	10
C5	Licences inutiles supprimées par application	Entretiens	50	50	50
C6	Coût mensuel moyen des licences par utilisateur	Entretiens	5 \$	5 \$	5 \$
<b>C7</b>	<b>Sous-total : frais de licence évités avec OIG</b>	<b>C4*C5*C6*12</b>	<b>30 000 \$</b>	<b>30 000 \$</b>	<b>30 000 \$</b>
C8	Coûts de conseil et d'assistance évités pour l'IAM	Entretiens	21 000 \$	25 000 \$	25 000 \$
Ct	Amélioration de l'efficacité de la plateforme et rationalisation logicielle	C3+C7+C8	251 000,00 \$	255 000,00 \$	255 000,00 \$
	Ajustement en fonction des risques	↓10 %			
Ctr	Amélioration de l'efficacité de la plateforme et rationalisation logicielle (valeur ajustée en fonction des risques)		225 900 \$	229 500 \$	229 500 \$
<b>Total sur trois ans : 684 900 \$</b>			<b>Valeur actuelle sur trois ans : 567 460 \$</b>		

## ACCROISSEMENT DE LA PRODUCTIVITÉ GRÂCE À L'AMÉLIORATION DE LA GOUVERNANCE DES ACCÈS

**Éléments probants et données.** Les personnes interrogées ont décrit comment OIG a rationalisé les flux de travail liés à l'accès pour les utilisateurs finaux, les responsables et les propriétaires d'applications. Avant OIG, les utilisateurs finaux formulaient souvent des demandes excessives, ce qui entraînait des retards et un suivi supplémentaire. Avec OIG, les demandes sont acheminées et résolues plus efficacement, ce qui réduit la charge de travail des demandeurs et des approuvateurs. L'automatisation et la simplification des demandes d'accès, des certifications et des examens des droits ont permis de réduire le temps passé à naviguer dans des interfaces obsolètes, à attendre des approbations manuelles ou à répondre à des processus de gouvernance incohérents.

- L'architecte de solutions informatiques dans le domaine des logiciels a déclaré : « [Avant OIG], il fallait entre 45 minutes et 2 heures pour obtenir les approbations, et jusqu'à 24 heures pour que l'accès soit accordé. Nous avons pu réduire ces délais à 30 minutes [pour] que la demande soit entièrement satisfaite de bout en bout ».
- Le directeur général des services financiers a déclaré à propos des demandes d'accès ou des modifications : « [Cela] aurait au moins pris le SLA de cinq jours ouvrables, et maintenant c'est automatisé et fait en 30 minutes. »

**Modélisation et hypothèses.** Compte tenu des informations recueillies lors des entretiens, Forrester émet les hypothèses suivantes concernant l'entreprise de référence :

- 5 000 utilisateurs finaux économisent, en moyenne, 2 heures par an avec OIG grâce à la diminution des problèmes d'accès et à l'amélioration des approbations d'accès et du provisionnement.
- Le salaire horaire moyen, toutes charges comprises, d'un utilisateur final est de 47 \$.

**Risques.** Le montant de ce bénéfice peut varier d'un client à l'autre en raison des différences suivantes :

- Les types et le volume des tâches liées aux accès attribuées aux utilisateurs professionnels.
- La maturité et la cohérence des flux de travail de gouvernance avant le déploiement d'OIG.
- Le niveau d'automatisation et de personnalisation appliqué pendant le déploiement.

- Le degré d'adoption des flux de travail de demande et de certification au sein de l'entreprise.
- Le salaire horaire moyen, toutes charges comprises, d'un utilisateur final.

**Résultats.** Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 15 %, et a ainsi obtenu une valeur actuelle (VA) totale ajustée en fonction des risques (taux d'actualisation de 10 %) de 497 000 \$ sur trois ans.

Valeur du temps gagné par les utilisateurs finaux grâce aux améliorations de la gouvernance des accès

**497 000 \$**

« OIG améliore considérablement l'expérience utilisateur. Ils peuvent désormais effectuer les tâches nécessaires en un temps réduit, puis se consacrer pleinement à leurs fonctions principales, [là où] auparavant, ces démarches entraînaient une perte considérable de productivité. »

DIRECTEUR, SERVICES FINANCIERS

Accroissement de la productivité grâce à l'amélioration de la gouvernance des accès					
Réf.	Indicateur	Source	Année 1	Année 2	Année 3
D1	Nombre total d'utilisateurs finaux	Entreprise de référence	5 000	5 000	5 000
D2	Nombre moyen d'heures économisées par utilisateur final grâce à l'amélioration des approbations d'accès et du provisionnement et à la diminution des problèmes d'accès avec OIG	Entretiens	2	2	2
D3	Salaire horaire, toutes charges comprises, d'un utilisateur final	Entreprise de référence	47 \$	47 \$	47 \$
D4	Productivité récupérée	Méthodologie TEI	50 %	50 %	50 %
Dt	Accroissement de la productivité grâce à l'amélioration de la gouvernance des accès	$D1 \cdot D2 \cdot D3 \cdot D4$	235 000 \$	235 000 \$	235 000 \$
	Ajustement en fonction des risques	↓ 15 %			
Dtr	Accroissement de la productivité grâce à l'amélioration de la gouvernance des accès (valeur ajustée en fonction des risques)		199 750 \$	199 750 \$	199 750 \$
<b>Total sur trois ans : 599 250 \$</b>			<b>Valeur actuelle sur trois ans : 496 749 \$</b>		

## RÉDUCTION DU RISQUE DE FAILLE DE SÉCURITÉ

**Éléments probants et données.** Les personnes interrogées ont confirmé qu'Okta Identity Governance contribuait à réduire le risque de violation de la sécurité en appliquant le principe du moindre privilège, en supprimant les droits inutiles et en automatisant les examens et les suppressions. Plusieurs ont souligné le rôle d'OIG dans la limitation de l'extension abusive des accès et le nettoyage des accès hérités, qu'ils considèrent comme une capacité fondamentale dans leur transition vers une architecture Zero Trust.

- Le directeur principal, responsable mondial de l'IAM dans une société de services professionnels, a déclaré qu'OIG a contribué à réduire les accès surprovisionnés et à minimiser les erreurs humaines, qui exposaient auparavant l'entreprise à des risques inutiles. « Les utilisateurs apprécient la séparation des tâches et la gestion des droits conflictuels. ... L'automatisation fournie par OIG analyse rapidement les rôles existants pour s'assurer que celui que vous demandez n'entre pas en conflit avec ceux que vous détenez déjà, et elle corrige le problème en amont, avant même l'attribution. C'est un enjeu majeur. »

## ANALYSE DES BÉNÉFICES

- Le directeur de la sécurité de l'information dans le secteur des soins de santé a expliqué qu'OIG a permis de réduire considérablement l'exposition aux risques liés aux informations de santé protégées (PHI). OIG a contribué à renforcer la gouvernance autour de l'accès aux PHI, en veillant à ce que seuls les utilisateurs essentiels aient accès aux données sensibles. Cette réduction ciblée des accès inutiles a permis d'atténuer les risques potentiels en matière de conformité et de sécurité.
- Le DSI d'une entreprise de services financiers a déclaré : « Le fait de pouvoir séparer les tâches et d'appliquer des politiques nous aide à prévenir les conflits d'intérêts et à réduire les risques de fraude. ... Nous avons constaté une réduction des menaces internes parce que nous avons beaucoup plus de visibilité sur les examens et les certifications d'accès, en particulier avec les sous-traitants et les partenaires tiers. L'automatisation du déprovisionnement garantit que nous ne laissons pas d'accès à d'anciens employés ou à d'anciens sous-traitants ou fournisseurs qui ont quitté l'entreprise, ce qui réduit le risque pour nous ».

**Modélisation et hypothèses.** Compte tenu des informations recueillies lors des entretiens, Forrester émet les hypothèses suivantes concernant l'entreprise de référence :

- L'entreprise de référence est exposée à un risque annuel de violation évalué à 3,027 millions de dollars.<sup>2</sup> La probabilité qu'elle soit victime d'une ou plusieurs violations est de 63 %.<sup>3</sup>
- Parmi ces violations, 76 % ont pour origine des attaques externes ou des incidents internes, ou sont liées à l'écosystème externe.<sup>4</sup>
- Quatre-vingt pour cent de ces incidents peuvent être résolus par une gouvernance des identités et des contrôles d'accès plus solides fournis par OIG.
- L'entreprise de référence réduit son exposition à ces risques de 10 % grâce à l'adoption d'OIG, sur la base des améliorations signalées par les personnes interrogées en matière d'hygiène des accès et d'efficacité de l'examen.

**Risques.** Le montant de ce bénéfice peut varier d'un client à l'autre en raison des différences suivantes :

- La taille de l'entreprise, le secteur d'activité et le profil de risque de sécurité inhérent.
  - La maturité et les outils de gouvernance des identités en place.
  - L'étendue du déploiement et de l'application des politiques d'accès d'OIG.
  - L'alignement interne entre les équipes chargées de l'IAM, de la sécurité et de la conformité.
-

**Résultats.** Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 20 %, obtenant ainsi une VA totale ajustée en fonction des risques (taux d'actualisation de 10 %) de 231 000 \$ sur trois ans.

« Nous avons considérablement amélioré notre posture de sécurité, ce qui satisfait notre RSSI, nos équipes de conformité et de gestion des risques, nos clients et nos actionnaires. [OIG] présente beaucoup d'avantages du point de vue de la sécurité. »

DSI, SERVICES FINANCIERS

### Réduction du risque de faille de sécurité

Réf.	Indicateur	Source	Année 1	Année 2	Année 3
E1	Coût cumulé des violations pour l'entreprise de référence	Étude Forrester	3 027 000 \$	3 027 000 \$	3 027 000 \$
E2	Probabilité que l'entreprise de référence subisse une ou plusieurs violations	Étude Forrester	63 %	63 %	63 %
E3	Pourcentage de violations provenant d'attaques externes ciblant les entreprises, d'incidents internes ou impliquant l'écosystème externe	Étude Forrester	76 %	76 %	76 %
E4	Pourcentage de ces attaques pouvant être traitées avec OIG	Étude Forrester	80 %	80 %	80 %
<b>E5</b>	<b>Sous-total : exposition annuelle au risque pouvant être traitée avec OIG</b>	<b>E1*E2*E3*E4</b>	<b>1 159 462,0 \$</b>	<b>1 159 462,0 \$</b>	<b>1 159 462,0 \$</b>
E6	Réduction des coûts liés au risque d'exposition à une violation pouvant être traitée avec OIG	Entretiens	10 %	10 %	10 %
Et	Réduction du risque de faille de sécurité	E5*E6	115 946 \$	115 946 \$	115 946 \$
	Ajustement en fonction des risques	↓20 %			
Etr	Réduction du risque d'une violation de la sécurité (valeur ajustée en fonction des risques)		92 757 \$	92 757 \$	92 757 \$
<b>Total sur trois ans : 278 270 \$</b>			<b>Valeur actuelle sur trois ans : 230 672 \$</b>		

### BÉNÉFICES NON QUANTIFIÉS

Les personnes interrogées ont mentionné d'autres avantages dont leurs entreprises ont bénéficié, mais qu'elles n'ont pas été en mesure de quantifier :

- **Délai de rentabilité rapide.** Les personnes interrogées ont constamment souligné la rapidité avec laquelle elles ont pu déployer et tirer parti d'OIG par rapport aux plateformes IGA traditionnelles qui nécessitaient souvent des mois de planification, de personnalisation et de travail d'intégration. OIG a permis aux équipes de mettre en place les fonctionnalités de base (notamment les demandes d'accès et les flux de certification) avec un minimum de ressources et d'efforts de configuration. Cette accélération a permis aux entreprises de commencer à réaliser des améliorations de gouvernance significatives presque immédiatement, avant même l'optimisation complète ou le déploiement à grande échelle.

Le DSI d'une entreprise de services financiers a noté qu'OIG a fourni un délai de valorisation plus rapide en raison de son intégration profonde avec l'infrastructure Okta existante de l'entreprise, notamment l'authentification unique, l'authentification multifactorielle et la gestion de l'accès aux API. Ces services de base étant déjà en place, OIG a pu être déployé plus rapidement et avec moins d'obstacles à l'intégration que les solutions concurrentes.

Le directeur de la sécurité de l'information dans le secteur des soins de santé a déclaré : « Le temps de déploiement était presque nul. ... Il n'y a vraiment rien à faire. Cela fait partie de la plateforme [Okta]. ... Nous l'avons mis en production en deux semaines, ce fut un véritable coup de maître pour nous ».

Le directeur principal, responsable mondial de l'IAM dans une entreprise de services professionnels, a évoqué le processus de déploiement : « Nous étions trois à l'époque, deux ingénieurs et moi et c'était tout, nous parlions au téléphone le jeudi et le vendredi, puis j'ai levé les yeux et j'ai réalisé que c'était fait. Nous avons des demandes d'accès. Nous avons une gouvernance et des certifications qui tournent maintenant. Passons à la production. Nous aurions pu le faire dès le premier jour si nous avions eu davantage confiance en nos capacités ».

- **Renforcement de la satisfaction des équipes informatiques et de sécurité.** Les personnes interrogées ont déclaré qu'en éliminant les tâches manuelles répétitives et en réduisant la charge administrative liée à la gestion des demandes d'accès et des

certifications, OIG a permis à leurs équipes de se concentrer sur des tâches plus stratégiques et à plus forte valeur ajoutée. Les personnes interrogées ont décrit cela comme un stimulant de la productivité *et* de la culture pour les équipes informatiques, de l'IAM et de la sécurité. Le directeur de l'architecture de sécurité dans un cabinet de conseil informatique a déclaré : « Maintenant, nous devons gérer moins de processus manuellement, et cela nous permet de nous concentrer sur des objectifs plus stratégiques ». Le directeur principal, responsable mondial de l'IAM dans une entreprise de services professionnels a déclaré : « Mes collaborateurs sont maintenant en train d'accéder à d'autres fonctions dont ils rêvaient et qu'ils voulaient exercer, mais pour lesquelles ils ne disposaient pas de CV. [OIG] permet à un dirigeant de hiérarchiser le travail différemment parce qu'il le confie à un membre de l'équipe qui non seulement veut l'effectuer en tant qu'analyste, mais en a réellement la volonté. Il frappe à votre porte, suppliant que vous lui confiez ce genre de travail. C'est le travail le plus cool qui soit ».

« L'expertise qu'apporte [Okta] est tout à fait louable. Je prends beaucoup de plaisir à travailler avec cette entreprise. Son personnel chargé de la réussite des clients et de l'assistance sait vraiment de quoi il parle. »

DIRECTEUR, SERVICES FINANCIERS

## FLEXIBILITÉ

La valeur de la flexibilité est propre à chaque client. Il existe de nombreux scénarios dans lesquels un client met Identity Governance en œuvre puis trouve par la suite d'autres possibilités d'utilisation et d'autres opportunités commerciales, notamment :

- **Amélioration de la pérennité et de l'agilité.** Les personnes interrogées ont mentionné la flexibilité d'OIG comme un facteur clé de succès à court terme et de croissance stratégique à long terme. Plusieurs personnes interrogées ont signalé qu'elles avaient commencé par un cas d'utilisation restreint, comme les demandes d'accès ou

l'intégration, et qu'elles avaient ensuite étendu la portée à d'autres applications, unités opérationnelles ou cadres de conformité. Elles ont décrit cette approche progressive comme essentielle pour aligner le champ d'application de la gouvernance sur l'état de préparation interne et l'évolution des priorités réglementaires. L'intégration native d'OIG avec la plateforme d'identité d'Okta a permis aux entreprises des personnes interrogées d'évoluer sans ajouter de charge administrative ni perturber les flux de travail existants ; les contrôles ont également pu être configurés pour prendre en charge diverses zones géographiques et normes (par exemple, SOX, HIPAA et ISO). Le directeur de la sécurité de l'information dans le secteur des soins de santé a résumé cela simplement : « [Avec OIG,] vous êtes maître de votre destin ».

Pour être quantifiée, la flexibilité doit faire partie d'un projet spécifique (ce point est décrit plus en détail dans la section [Approche Total Economic Impact](#)).

« L'outil, le soutien, le mécanisme qu'ils ont mis en place pour soutenir l'outil - c'est ultra-flexible. »

DIRECTEUR PRINCIPAL, RESPONSABLE MONDIAL DE L'IAM, SERVICES PROFESSIONNELS

# Analyse des coûts

Données relatives aux coûts quantifiés appliquées à l'entreprise de référence

Total des coûts							
Réf.	Coût	Situation initiale	Année 1	Année 2	Année 3	Total	Valeur actuelle
Dtr	Frais liés à OIG	0 \$	330 000 \$	330 000 \$	330 000 \$	990 000 \$	820 661 \$
Etr	Formation, déploiement et optimisation	27 878 \$	0 \$	0 \$	0 \$	27 878 \$	27 878 \$
	Total des coûts (valeurs ajustées en fonction des risques)	27 878 \$	330 000 \$	330 000 \$	330 000 \$	1 017 878 \$	848 539 \$

## FRAIS LIÉS A OIG

**Éléments probants et données.** Les personnes interrogées ont fourni des détails sur les coûts corroborés par Okta. Pour l'entreprise de référence, une estimation des coûts de 5 \$ par utilisateur et par mois est basée sur la mise en œuvre et le scénario spécifiques liés à l'entreprise de référence. Les coûts réels actualisés varieront en fonction des services fournis avec Okta et OIG à un client particulier. Veuillez contacter Okta pour plus d'informations.

**Modélisation et hypothèses.** Compte tenu des informations recueillies lors des entretiens, Forrester émet les hypothèses suivantes concernant l'entreprise de référence :

- OIG est déployé pour 5 000 identités gérées.
- Les frais mensuels se montent à 5 \$ par identité.

**Risques.** Ce coût peut varier d'un client à l'autre en raison des différences de tarification négociée et de structure de licence.

**Résultats.** Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 10 %, obtenant ainsi une VA totale ajustée en fonction des risques (taux d'actualisation de 10 %) de 821 000 \$ sur trois ans.

Frais liés à OIG						
Réf.	Indicateur	Source	Situation initiale	Année 1	Année 2	Année 3
F1	Identités gérées avec OIG	Entreprise de référence		5 000	5 000	5 000
F2	Frais mensuels d'OIG par identité	Entretiens		5 \$	5 \$	5 \$
Ft	Frais liés à OIG	F1*F2*12	0 \$	300 000 \$	300 000 \$	300 000 \$
	Ajustement en fonction des risques	↑10 %				
Ftr	Frais liés à OIG (valeurs ajustées en fonction des risques)		0 \$	330 000 \$	330 000 \$	330 000 \$
<b>Total sur trois ans : 990 000 \$</b>			<b>Valeur actuelle sur trois ans : 820 661 \$</b>			

## FORMATION, DÉPLOIEMENT ET OPTIMISATION.

**Éléments probants et données.** Les personnes interrogées ont signalé que certaines activités de formation, de déploiement et d'optimisation étaient nécessaires pour configurer OIG, former le personnel et affiner les flux de travail d'accès. Ces activités ont duré de quelques semaines à quelques mois.

**Modélisation et hypothèses.** Compte tenu des informations collectées lors des entretiens, Forrester émet les hypothèses suivantes concernant l'entreprise de référence :

- L'équipe chargée de l'IAM et le personnel de soutien dédié à l'audit et à la conformité passent huit semaines à déployer OIG, en allouant en moyenne 10 % du temps aux tâches spécifiques à OIG.
- Le salaire horaire moyen, toutes charges comprises, d'un ETP IAM, d'audit et de conformité est de 66 \$.

**Risques.** Le montant de cette dépense peut varier d'un client à l'autre en raison des différences suivantes :

- La taille et le niveau d'expérience de l'équipe chargée de l'IAM interne.
- La complexité des systèmes et des intégrations existants.
- Le salaire horaire moyen, toutes charges comprises, d'un ETP IAM, d'audit et de conformité.

## ANALYSE DES COÛTS

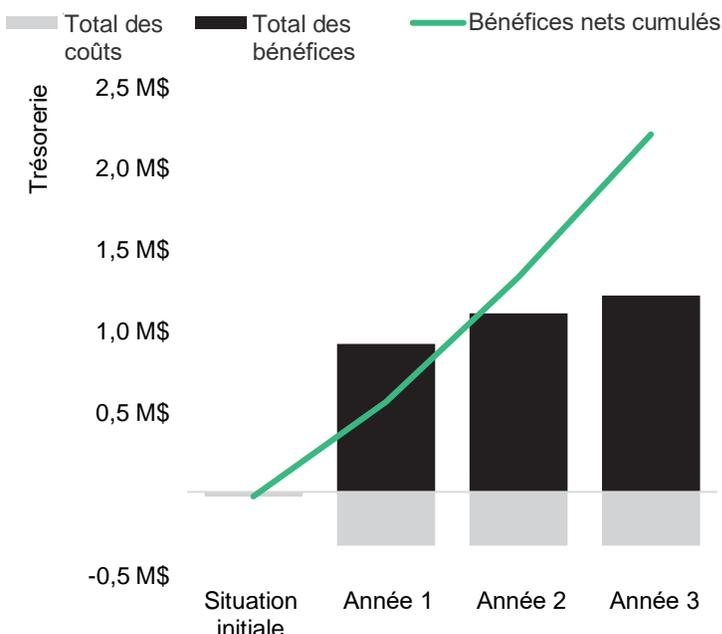
**Résultats.** Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 10 %, obtenant ainsi une VA totale ajustée en fonction des risques (taux d'actualisation de 10 %) de 28 000 \$ sur trois ans.

<b>Formation, déploiement et optimisation</b>						
<b>Réf.</b>	<b>Indicateur</b>	<b>Source</b>	<b>Situation initiale</b>	<b>Année 1</b>	<b>Année 2</b>	<b>Année 3</b>
G1	ETP IAM et ETP dédiés à l'audit/à la conformité	Entreprise de référence	12			
G2	Période d'intégration (en semaines)	Entretiens	8			
G3	Temps moyen alloué à la formation, au déploiement et/ou à l'optimisation d'OIG	Entretiens	10 %			
<b>G4</b>	<b>Sous-total : heures consacrées à l'intégration d'OIG</b>	<b>G1*G2*40*G3</b>	<b>384</b>			
G5	Taux horaire toutes charges comprises d'un IAM et d'un ETP dédié à l'audit/à la conformité	Entreprise de référence	66 \$			
Gt	Formation, déploiement et optimisation	G4*G5	25 344 \$	0 \$	0 \$	0 \$
	Ajustement en fonction des risques	↑10 %				
Gtr	Formation, déploiement et optimisation (valeur ajustée en fonction des risques)		27 878 \$	0 \$	0 \$	0 \$
<b>Total sur trois ans : 27 878 \$</b>			<b>Valeur actuelle sur trois ans : 27 878 \$</b>			

# Bilan financier

Indicateurs consolidés sur trois ans et ajustés en fonction des risques

**Graphique de trésorerie  
(valeurs ajustées en fonction des risques)**



Les résultats financiers calculés dans les sections Bénéfices et Coûts peuvent être utilisés pour déterminer le retour sur investissement (ROI), la valeur actuelle nette (VAN) et le délai de rentabilisation de l'entreprise de référence. Forrester se base sur un taux d'actualisation annuel de 10 % pour cette analyse.

Ces ROI, VAN et délai de rentabilisation ajustés en fonction des risques s'obtiennent en appliquant des facteurs d'ajustement aux résultats bruts des sections Bénéfices et Coûts.

## Analyse des flux de trésorerie (valeurs ajustées en fonction des risques)

	Situation initiale	Année 1	Année 2	Année 3	Total	Valeur actuelle
Total des coûts	(27 878 \$)	(330 000 \$)	(330 000 \$)	(330 000 \$)	(1 017 878 \$)	(848 539 \$)
Total des bénéfices	0 \$	911 173 \$	1 096 688 \$	1 208 320 \$	3 216 181 \$	2 642 522 \$
Bénéfices nets	(27 878 \$)	581 173 \$	766 688 \$	878 320 \$	2 198 303 \$	1 793 983 \$
ROI						211 %
Délai de récupération						< 6 mois

## **ANNEXE A : TOTAL ECONOMIC IMPACT**

La méthodologie Total Economic Impact (TEI) a été développée par Forrester Research pour améliorer les processus de décision des entreprises en matière de technologie et pour aider les fournisseurs à communiquer avec leur clientèle sur la valeur de leurs produits et services. Elle aide aussi les entreprises à démontrer, justifier et valoriser les initiatives IT auprès de leur direction et des autres parties prenantes.

### **Approche Total Economic Impact**

Les bénéfices représentent la valeur que le produit apporte à l'entreprise. La méthodologie TEI pondère les bénéfices et les coûts de la même manière, ce qui permet d'examiner pleinement l'impact de la technologie sur l'ensemble de l'entreprise.

Les coûts tiennent compte de toutes les dépenses nécessaires pour apporter la valeur proposée ou les bénéfices du produit. La catégorie Coûts du TEI correspond aux coûts incrémentaux par rapport à l'environnement existant pour les coûts récurrents liés à la solution.

La flexibilité désigne la valeur stratégique qui peut être obtenue pour un futur investissement en complément de l'investissement initial. La possibilité de tirer parti de cet avantage présente une VA qui peut être estimée.

Les risques mesurent l'incertitude des estimations de bénéfices et de coûts en considérant : 1) la probabilité que les estimations correspondent aux projections initiales et 2) la probabilité que les estimations soient mesurées dans le temps. Les facteurs de risque de la méthode TEI reposent sur une « distribution triangulaire ».

### **Valeur actuelle (VA)**

Valeur actuelle ou courante des futurs mouvements de trésorerie nets (actualisés) à un taux d'intérêt donné (taux d'actualisation). La VA des coûts et des bénéfices entre dans la VAN totale des flux de trésorerie.

### **Valeur actuelle nette (VAN)**

Valeur actuelle ou courante des futurs flux de trésorerie nets (actualisés) à un taux d'intérêt donné (taux d'actualisation). La VAN positive d'un projet indique normalement que l'investissement est recommandé, à moins que d'autres projets ne présentent des VAN supérieures.

## **Retour sur investissement (ROI)**

Rentabilité attendue d'un projet, exprimée en pourcentage. Le ROI se calcule en divisant les bénéfices nets (bénéfices moins coûts) par les coûts.

## **Taux d'actualisation**

Taux d'intérêt utilisé dans l'analyse des flux de trésorerie pour prendre en compte la valeur temps de l'argent. Les entreprises utilisent généralement des taux d'actualisation compris entre 8 et 16 %.

## **Délai de récupération**

Seuil de rentabilité d'un investissement. Il s'agit du moment où les bénéfices nets (déduction faite des coûts) sont égaux à l'investissement ou au coût initial.

La colonne indiquant l'investissement initial présente les coûts engagés à « l'instant 0 » ou au début de l'Année 1, et non actualisés. Tous les autres mouvements de trésorerie se voient appliquer le taux d'actualisation en fin d'année. Les calculs de la VA sont effectués pour chaque estimation des coûts et des bénéfices totaux. Les calculs de la VAN qui figurent dans les tableaux de synthèse correspondent à la somme de l'investissement initial et des mouvements de trésorerie actualisés chaque année. Il est possible que les calculs des sommes et de la valeur actuelle des tableaux Total des bénéfices, Total des coûts et Mouvements de trésorerie ne correspondent pas exactement, certains nombres pouvant avoir été arrondis.

## ANNEXE B : NOTES DE FIN

---

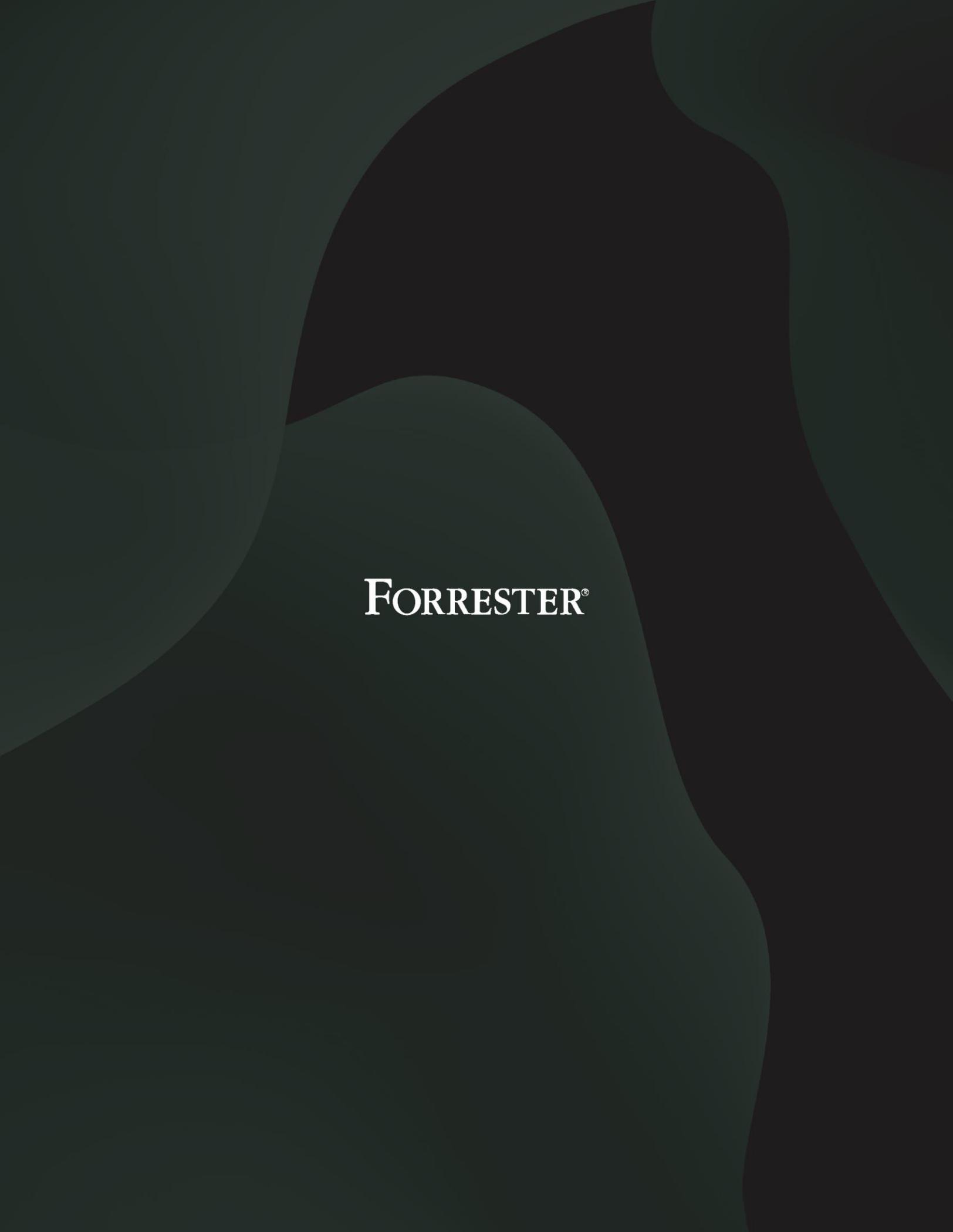
<sup>1</sup>La méthodologie Total Economic Impact (TEI) a été développée par Forrester Research pour améliorer les processus de prise de décision des entreprises en matière de choix technologique et pour aider les fournisseurs de solutions à communiquer leur proposition de valeur aux clients. La méthodologie TEI aide les entreprises à démontrer, justifier et concrétiser la valeur tangible des initiatives commerciales et technologiques auprès de la direction et des autres parties prenantes clés de l'entreprise.

<sup>2</sup>Analyse de régression des coûts cumulés totaux déclarés pour toutes les violations subies par les entreprises des décideurs en matière de sécurité au cours des 12 derniers mois. Le chiffre d'affaires de l'entreprise de référence est utilisé comme donnée d'entrée dans la formule de régression. Source : enquête de Forrester sur la sécurité, 2024. « Selon votre meilleure estimation, quel a été le coût total cumulé de toutes les atteintes à la sécurité subies par votre entreprise au cours des 12 derniers mois ? » Base : 1 660 décideurs mondiaux en matière de sécurité ayant été confrontés à une violation au cours des 12 derniers mois.

<sup>3</sup>Analyse de régression de la probabilité de subir une ou plusieurs violations, en utilisant la fréquence à laquelle les entreprises ont subi des violations au cours des 12 derniers mois, telle que rapportée par les responsables de la sécurité. Le chiffre d'affaires de l'entreprise de référence est utilisé comme donnée d'entrée dans la formule de régression. Source : enquête de Forrester sur la sécurité, 2024. « Combien de fois estimez-vous que les données sensibles de votre entreprise ont été potentiellement compromises ou violées au cours des 12 derniers mois ? » Base : 2 769 décideurs mondiaux en matière de sécurité.

<sup>4</sup>Pourcentage des violations par vecteur d'attaque principal, tel que rapporté par les décideurs en matière de sécurité dont les entreprises ont subi au moins une violation au cours des 12 derniers mois. Source : enquête de Forrester sur la sécurité, 2024 « Parmi les cas où les données sensibles de votre entreprise ont été potentiellement compromises ou violées au cours des 12 derniers mois, veuillez indiquer combien d'entre eux entrent dans chacune des catégories ci-dessous. » Base : 1 542 décideurs mondiaux en matière de sécurité ayant été confrontés à une violation au cours des 12 derniers mois.

---

The image features a dark green background with several overlapping, organic, wavy shapes in varying shades of green and dark teal. The word "FORRESTER" is centered in a white, serif font with a registered trademark symbol. The overall aesthetic is professional and modern.

FORRESTER®