Enterprise Strategy Group™
Par TechTarget

UNE SÉCURITÉ ULTRAPERFORMANTE
pour les environnements hybrides et multicloud et la croissance de l'entreprise

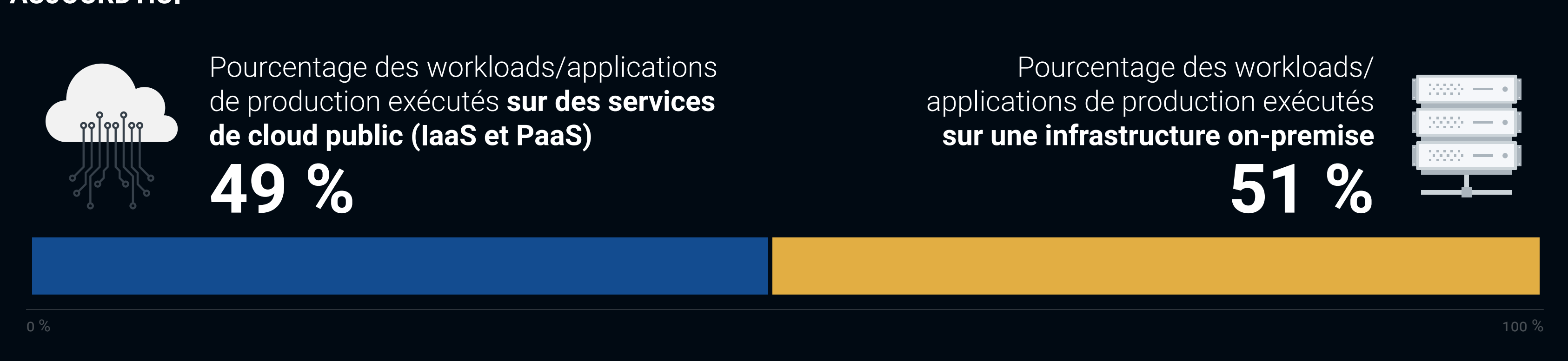
Aujourd'hui, les entreprises doivent non seulement passer au numérique pour optimiser leur productivité et leur capacité d'innovation, mais aussi instaurer une sécurité qui couvre leurs workloads dans les environnements hybrides et multicloud. Cisco les aide à moderniser leurs programmes de sécurité afin de protéger les applications absolument partout, en accélérant le développement et la croissance de l'activité.

Cette infographie d'Enterprise Strategy Group a été créée à la demande de Cisco et est distribuée avec l'autorisation de TechTarget Inc.

L'importance d'une sécurité capable de couvrir les applications dans les environnements distribués

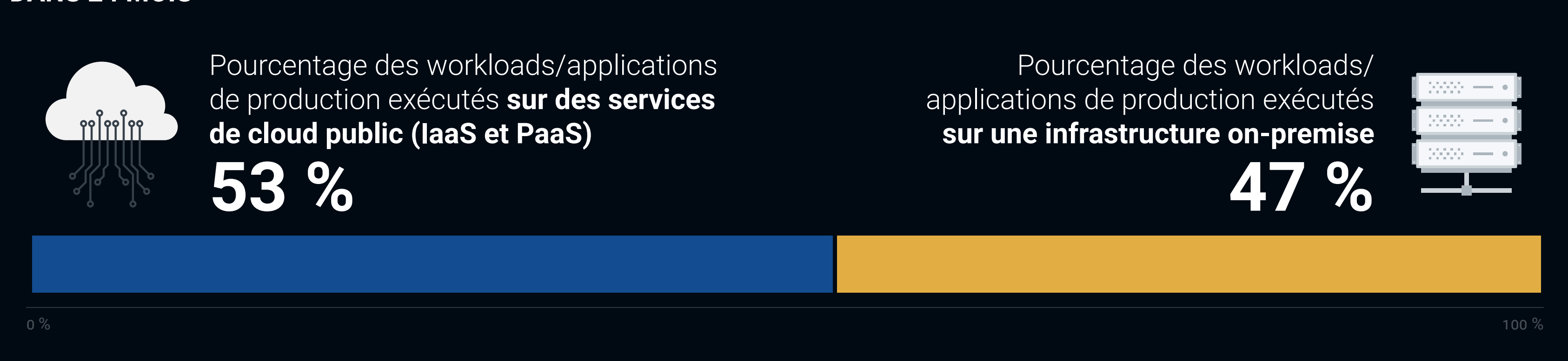
Les entreprises s'appuient massivement sur les clouds publics pour exploiter des plateformes informatiques de pointe sans se soucier de la couche sous-jacente ni de la maintenance. Par ailleurs, elles doivent également prendre en charge leurs applications dans les environnements on-premise. Il est donc difficile pour les équipes responsables de la sécurité d'accompagner la migration vers les services cloud et de gérer les workloads distribués entre plusieurs plateformes cloud et environnements on-premise.

AUJOURD'HUI


Pourcentage des workloads/applications de production exécutés **sur des services de cloud public (IaaS et PaaS)**
49 %

Pourcentage des workloads/applications de production exécutés **sur une infrastructure on-premise**
51 %

DANS 24 MOIS


Pourcentage des workloads/applications de production exécutés **sur des services de cloud public (IaaS et PaaS)**
53 %

Pourcentage des workloads/applications de production exécutés **sur une infrastructure on-premise**
47 %

> La majorité (63 %) des entreprises font appel à **au moins trois** fournisseurs de services cloud (CSP). »
>
> *- **Melinda Marks,** Directrice, Cybersécurité, Enterprise Strategy Group*

La sécurité figure en tête de liste des difficultés rencontrées dans le cadre d'une collaboration avec plusieurs CSP, suivie par les problèmes relatifs à l'évolutivité ainsi qu'à la garantie des performances et de la disponibilité des applications.

31 %
Respect des exigences de sécurité

30 %
Gestion de différentes API

29 %
Intégration et mise à disposition continues (pipeline CI/CD)

26 %
Différences/disponibilité des interconnexions de réseaux

26 %
Mise en œuvre d'une méthodologie de déploiement cohérente

Pour les migrations vers le cloud, la sécurité constitue la principale préoccupation, suivie par le coût et le temps.

25 %
Respect des exigences de sécurité

25 %
Respect des contraintes budgétaires

25 %
Temps et coût pour se former à différentes architectures

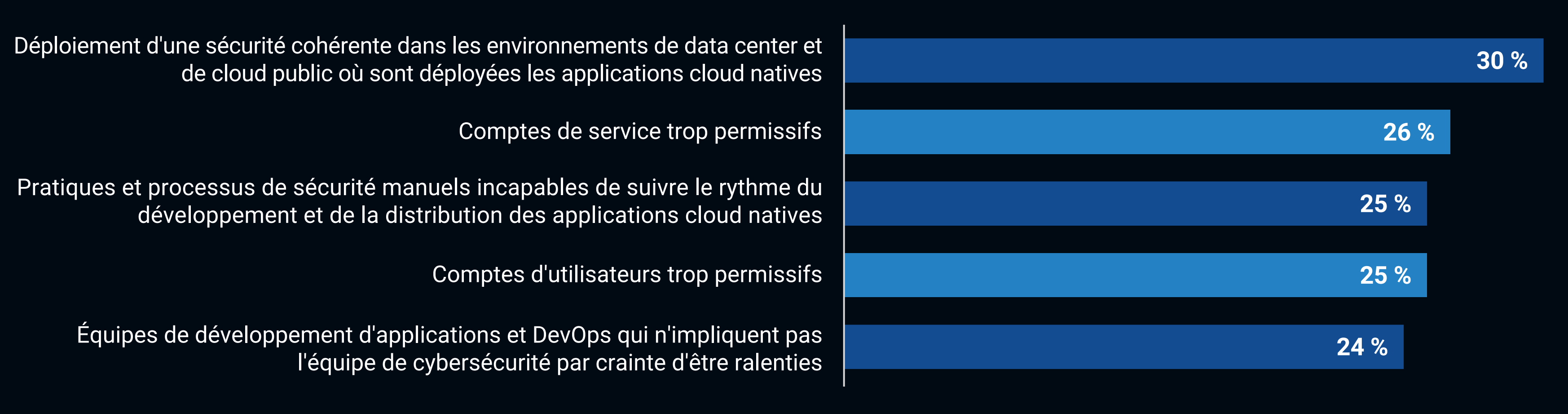
24 %
Différences/disponibilité des interconnexions de réseaux

26 %
Temps et efforts investis pour déplacer les applications/données entre divers services de cloud public

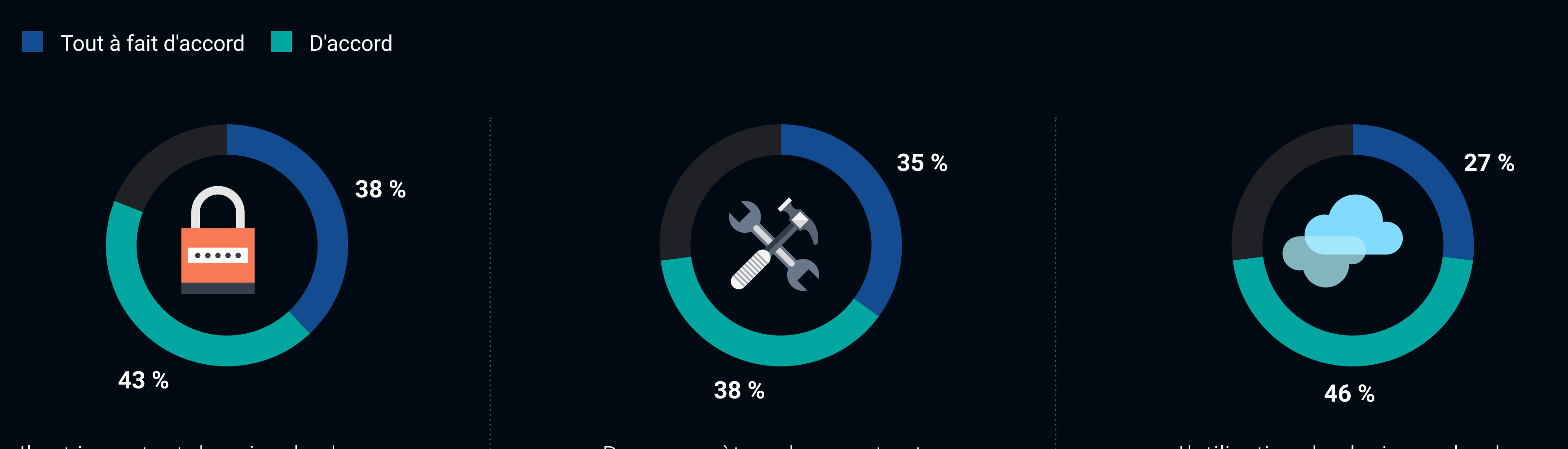
Une stratégie de sécurité efficace pour stimuler la croissance

Les équipes de sécurité ne doivent pas bloquer la croissance et l'innovation, mais au contraire les favoriser. Il en va de même pour l'évolutivité des applications. Cette tâche délicate exige notamment une gestion efficace des risques, une protection complète des applications dans les différents environnements ainsi qu'une fine adaptation des programmes de sécurité.

Les plus grands défis de la sécurité cloud concernent la cohérence, les autorisations et l'évolutivité.



Les trois principaux défis autour de la gestion de la sécurité dans l'ensemble des environnements



Il est important de suivre les bonnes pratiques de sécurité du secteur pour renforcer la protection.

Des paramètres de comptes trop permissifs engendrent des risques considérables en matière de sécurité et de conformité.

L'utilisation de plusieurs clouds publics complique le maintien d'une protection cohérente dans tous les environnements.

Passer d'un amoncellement d'outils cloisonnés à une solution axée sur l'efficacité

Les entreprises utilisent actuellement un trop grand nombre d'outils de sécurité distincts qui compliquent la vie de leurs équipes. Elles devraient plutôt adopter une approche qui les unifie, en offrant une visibilité sur les applications dans tous les environnements à l'aide d'un cadre dynamique interconnecté. Une telle stratégie améliore l'efficacité des opérations de sécurité grâce à des informations contextuelles sur les ressources qui limitent les risques et accélèrent la riposte aux incidents.

Un arsenal d'outils pour effectuer l'inventaire des ressources

52 %
Systèmes de gestion des ressources informatiques

40 %
Technologie de gestion de la surface d'exposition aux attaques des cyberressources

37 %
Sécurité des terminaux

34 %
Analyse du réseau

33 %
Outils de gestion de la sécurité du cloud

33 %
Gestion des terminaux

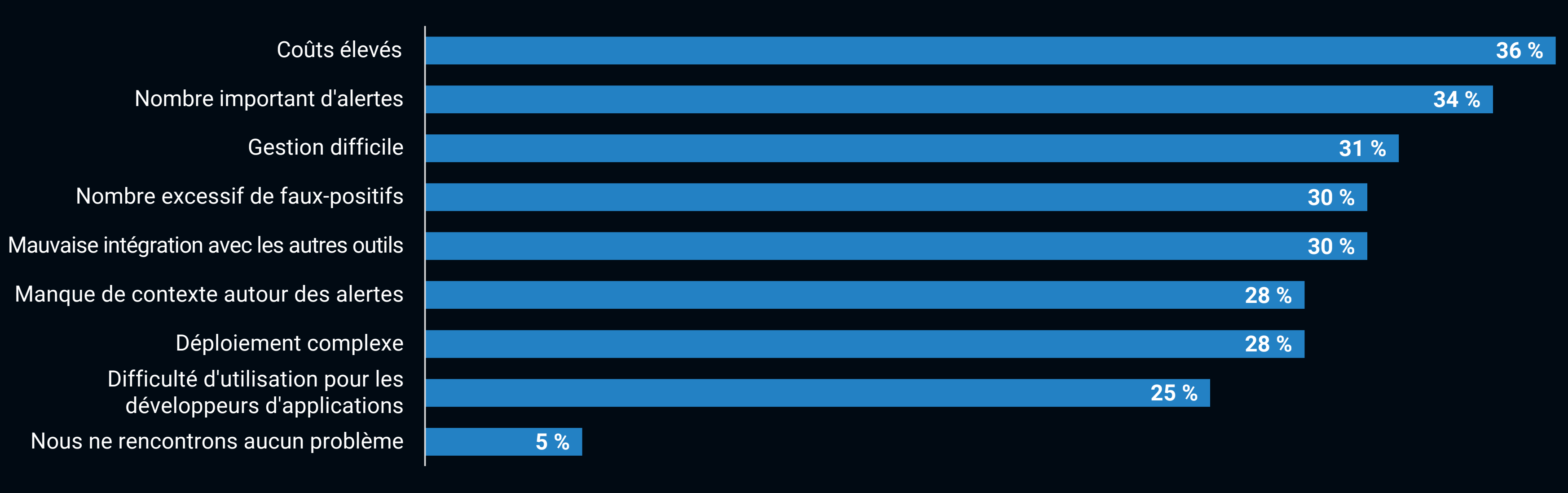
32 %
Outils d'évaluation/d'analyse des vulnérabilités

26 %
Contrôles d'accès réseau

26 %
Gestion des correctifs et de la configuration

25 %
Plateforme de gestion externe de la surface d'exposition aux attaques

Problèmes générés par l'utilisation de plusieurs solutions de protection des applications web



Les quatre principaux défis de gestion découlant de l'utilisation de plusieurs outils de sécurité dans différents environnements

45 %
Chaque technologie de sécurité requiert une formation distincte et possède des caractéristiques de mise en œuvre, de gestion et d'exploitation différentes, ce qui met à rude épreuve les ressources de l'entreprise.

36 %
Il est difficile d'obtenir une vue d'ensemble du niveau de sécurité lorsqu'il y a trop de technologies disparates.

33 %
Lorsque les équipes responsables de la sécurité doivent rassembler les données provenant de plusieurs outils de sécurité indépendants pour opérer, tout devient complexe et chronophage.

30 %
L'entreprise ne dispose pas du personnel et des compétences nécessaires pour gérer correctement ses technologies de sécurité.

Les entreprises sont en quête d'un moyen efficace de gérer la sécurité dans l'ensemble de leurs environnements à travers des processus et des contrôles cohérents permettant de protéger les applications absolument partout. De leur côté, les équipes responsables de la sécurité disposent alors de la flexibilité nécessaire pour s'adapter à la croissance de l'activité.

Les piliers d'un programme de sécurité efficace

Une visibilité totale sur l'ensemble des environnements et des ressources (réseau, applications et clouds) qui fournit un aperçu complet du niveau de sécurité.

Des informations contextuelles qui améliorent l'efficacité de la remédiation grâce à une évaluation des risques hiérarchisant les détections de vulnérabilités dans l'ensemble des environnements afin de mettre en œuvre les mesures les plus adéquates.

Des contrôles unifiés et cohérents qui permettent d'appliquer uniformément des politiques et des cadres de sécurité aux workloads dans l'ensemble des environnements.

Une protection complète des workloads qui préserve l'intégrité du trafic sur le réseau, les clouds et les VPC via une macro et une microsegmentation à la fois précises et cohérentes dans tous les environnements pour bloquer les mouvements latéraux non autorisés et ainsi protéger tant les données que les applications.

La suite Cisco Cloud Protection propose une approche moderne de la sécurité des applications ainsi qu'une protection de bout en bout pour les environnements hybrides et multicloud. Que ce soit pour des serveurs dédiés ou des infrastructures cloud natives, elle assure la sécurité complète des applications et protège les workloads dans tous les environnements, on-premise comme cloud.

cisco

En savoir plus

Source : résultats de l'enquête menée par Enterprise Strategy Group (ESG), *rapport d'étude sur le cloud distribué : L'état de la modernisation de l'infrastructure dans le cloud distribué*, août 2023
Source : rapport d'étude Enterprise Strategy Group (ESG), *Tendances de gestion de l'intégrité et des droits d'accès au cloud*, avril 2023
Source : rapport d'étude Enterprise Strategy Group (ESG), *La gestion de l'intégrité et de la sécurité demeure décentralisée et complexe*, juillet 2023
Source : résultats de l'enquête menée par Enterprise Strategy Group (ESG), *rapport d'étude ESG/ISSA sur les technologies et processus de cybersécurité*, juin 2022