Mai 2021

ÉTUDE DE MARCHÉ

La sécurité des applications : état des lieux en 2021

Les bots malveillants, les API défaillantes et les attaques contre les chaînes logistiques exposent les données des entreprises. »

Barracuda
Your journey, secured.

Sommaire

Introduction - La sécurité des applications : état des lieux en 2021 3

Les principaux défis 4-7

Les attaques de bots 8-11

La sécurité des API 12-16

Les attaques contre les chaînes logistiques 17-19

Conclusion 20

Barracuda en quelques mots 21

Introduction

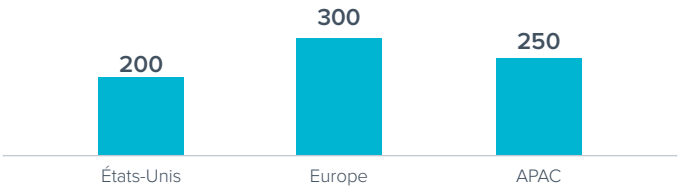
La sécurité des applications : état des lieux en 2021

La sécurité des applications donne du fil à retordre aux entreprises. Au fil des ans, les applications Web sont devenues le principal vecteur d'attaque, une tendance qui s'est accentuée avec le passage au télétravail en 2020. En effet, de nombreuses entreprises ont été contraintes d'exposer leurs applications internes à Internet et/ou de rapidement transférer leurs applications vers le cloud.

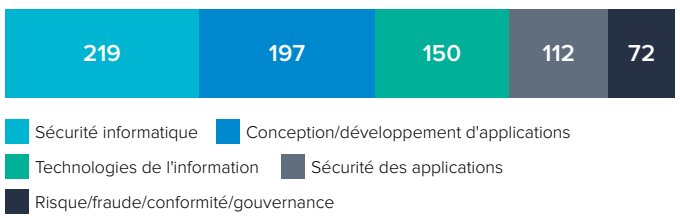
Dans le cadre de cette enquête, nous avons demandé aux entreprises le nombre d'intrusions qu'elles avaient subies au cours de l'année écoulée en raison d'une vulnérabilité liée à l'une de leurs applications. La moyenne mondiale était de deux intrusions au cours des 12 derniers mois.

Les personnes interrogées ont signalé que la grande majorité de ces attaques étaient dues à des vulnérabilités dans les applications Web. Les attaques de bots et celles contre les API ou encore les chaînes logistiques logicielles étaient les principales responsables de ces violations. Les participants reconnaissent que des améliorations significatives sont nécessaires dans ces trois domaines ; une tendance relativement homogène au niveau mondial, malgré quelques différences régionales et locales intéressantes.

Réponses par région



Réponses par poste



Méthodologie

Barracuda a fait appel à Vanson Bourne, une entreprise indépendante spécialisée en études de marché, pour mener une enquête mondiale auprès de **750 décideurs responsables du développement et de la sécurité des applications** au sein leur entreprise. Originaires des **États-Unis, d'Europe et de la région Asie-Pacifique**, les participants représentaient des entreprises comptant au moins 500 employés dans le monde. Dans la mesure où les responsabilités informatiques et les menaces de cybersécurité varient d'une région à l'autre, nous avons interrogé des personnes occupant divers postes dans différents secteurs d'activité afin d'obtenir une vision aussi fidèle que possible des risques liés à la sécurité des applications. L'enquête a été menée en mars et avril 2021.

Les principaux défis

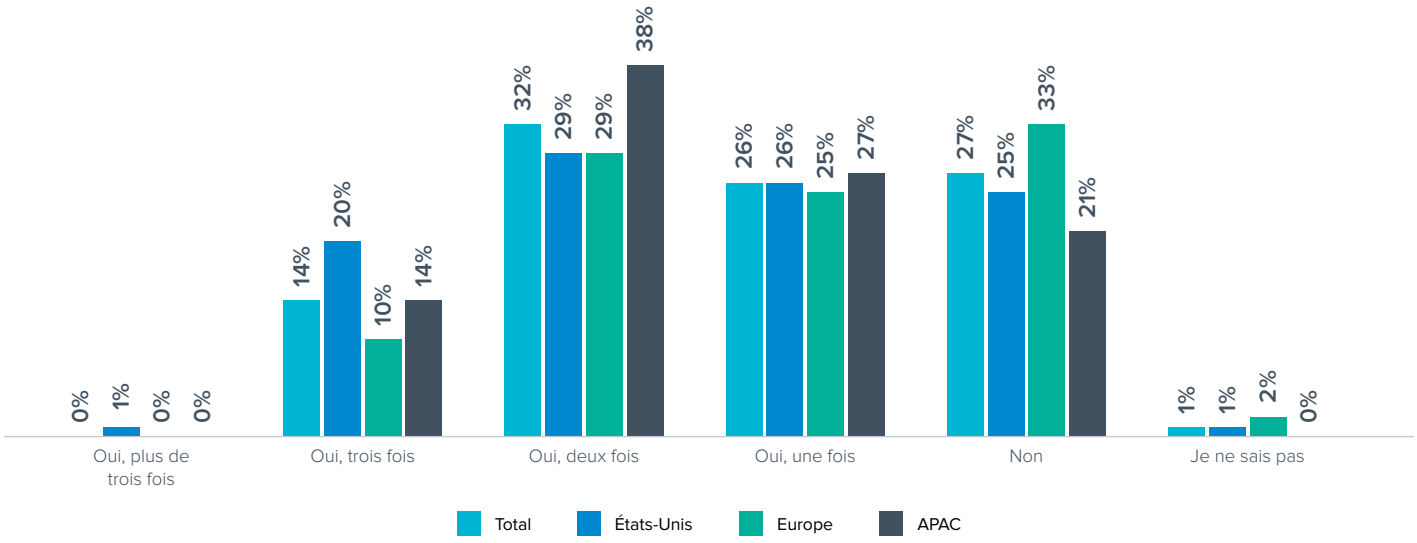
CONSTATATION Nº 1

Les entreprises interrogées ont subi en moyenne deux violations au cours des 12 derniers mois en raison d'une vulnérabilité liée à une application.

Avec 72 % des personnes ayant déclaré que leur entreprise avait subi au moins une violation de sécurité en raison d'une vulnérabilité liée à une application, force est de constater que les cyberattaques basées sur les applications ont gagné en agressivité et en ampleur. Cela s'explique probablement par la grande diversité de menaces de sécurité utilisées pour nuire aux entreprises et par les difficultés internes auxquelles beaucoup d'entre elles sont confrontées.

Au cours des 12 derniers mois, votre entreprise a-t-elle subi une violation de sécurité imputable à une vulnérabilité dans l'une de ses applications ?

(n=750)



Les principaux défis

CONSTATATION N° 2

Les défis que rencontrent les entreprises dans le domaine de la sécurité des applications dépassent les difficultés liées à la sécurisation des différents vecteurs d'attaque.

Alors que les entreprises sont manifestement en proie à des menaces de sécurité touchant leurs applications, notamment les attaques de bots et celles visant les chaînes logistiques logicielles ou encore les API, il en existe bien d'autres. Les exigences de rendement posent également problème, comme en témoignent les 35 % de personnes qui déclarent que l'intégration de la sécurité ralentit considérablement le développement des applications.

Au niveau mondial, les cinq principales difficultés rencontrées sont les bots, les attaques contre les chaînes logistiques, la détection des vulnérabilités, la sécurité des API et la sécurité ralentissant le développement des applications.

On observe quelques disparités régionales intéressantes. Aux États-Unis, la détection des vulnérabilités est absente du top 5. En revanche, la mise en œuvre de la sécurité dans les pratiques de CI/CD est souvent citée.

L'Europe, pour sa part, est moins préoccupée par les attaques visant les chaînes logistiques et le ralentissement du développement dû à l'intégration de la sécurité. C'est la neutralisation des menaces qui constitue le plus grand défi.

Dans la région Asie-Pacifique, le ralentissement du développement dû à l'intégration de la sécurité est une préoccupation beaucoup plus importante que dans les autres régions.

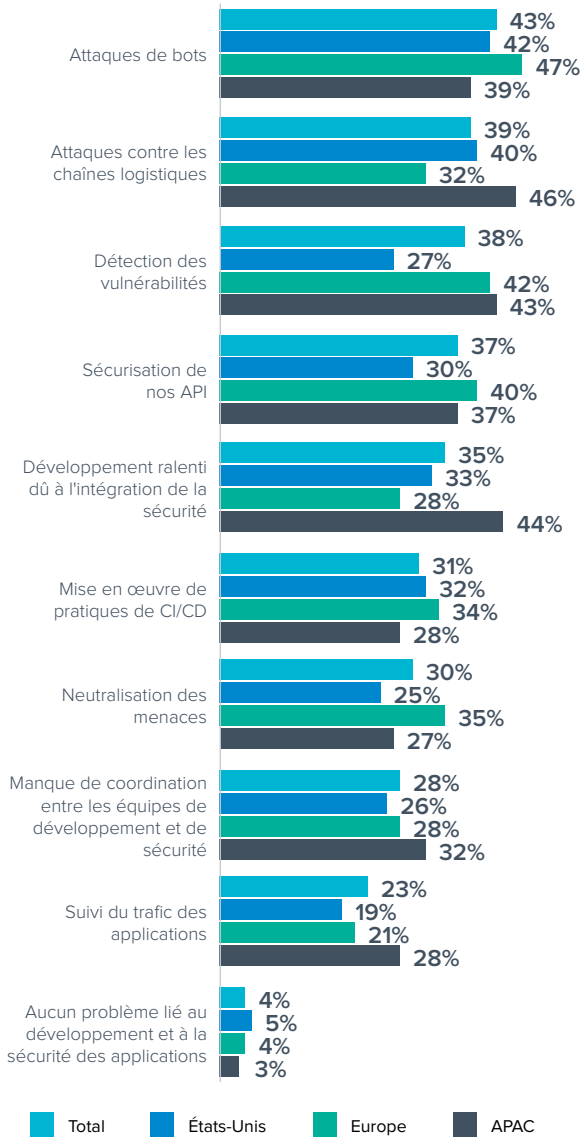
La détection des vulnérabilités pose problème avec de nombreuses solutions relativement avancées du marché, et la mise en œuvre de la sécurité au cours de la phase de développement, en particulier dans les environnements DevOps, constitue une tâche relativement complexe.

Dans ce rapport, nous nous concentrons sur les nouveaux défis suivants :

- Les bots
- Les attaques contre les chaînes logistiques
- La sécurité des API

Lesquelles de ces difficultés votre entreprise rencontre-t-elle dans le développement et la sécurité des applications ?

(n=750)



Les principaux défis

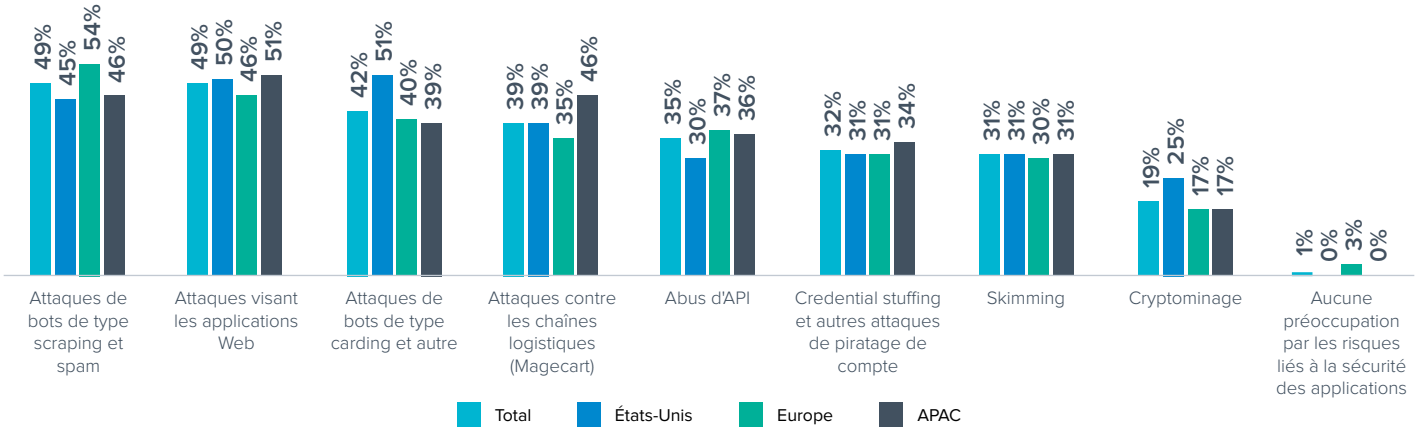
CONSTATATION N° 3

Les entreprises se préoccupent du large éventail de risques liés à la sécurité de leurs applications, et tout particulièrement de la diversité des attaques basées sur les bots.

Chacun sait que les bots sont devenus un problème récurrent pour les entreprises ces dernières années, comme en témoigne le fait que les attaques de bots constituent deux des trois risques de sécurité des applications les plus fréquemment cités par les décideurs. Ils sont suivis de près par les attaques visant les chaînes logistiques et les API. Les entreprises se doivent de garder à l'esprit toute l'importance de la sécurité des applications : l'une de ces menaces peut aisément exploiter une vulnérabilité et possiblement semer le chaos. Pour preuve, de nombreux répondants ont cité les vulnérabilités des applications Web/les attaques zero-day comme l'une des principales menaces.

Quels sont les risques liés à la sécurité des applications qui vous préoccupent le plus au sein de votre entreprise ?

(n=750)



Les attaques de bots

CONSTATATION N° 4

La diversité des attaques de bots capables d'exploiter les vulnérabilités des applications est un véritable fléau.

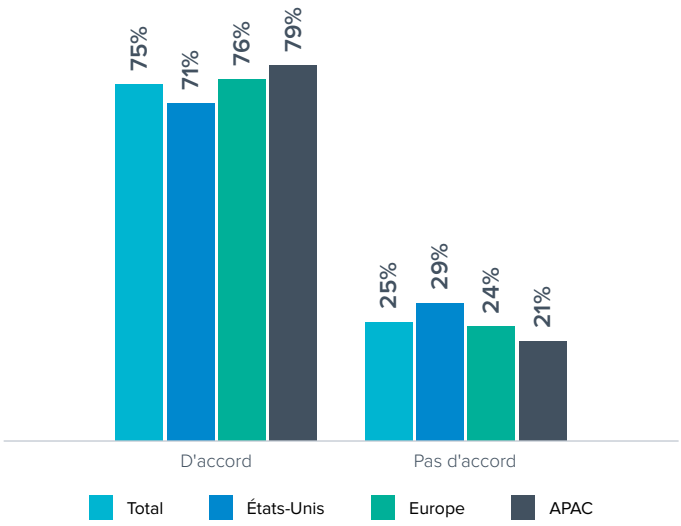
Trois quarts des décideurs reconnaissent que la diversité des attaques de bots pose de réelles difficultés à leur entreprise en ce qui concerne la protection des applications. Les entreprises semblent tout simplement totalement dépassées. Compte tenu de l'existence de toute une économie de bots en ligne, avec des marchés et des courtiers qui veillent à ce que les utilisateurs ne se fassent pas escroquer, ce phénomène ne peut que s'amplifier dans les années à venir. Les attaques automatisées couvrent une telle variété de vecteurs et de techniques qu'elles sont devenues un problème majeur dans le monde entier.

Les entreprises auront besoin de l'aide externe de fournisseurs experts en bots et en sécurité des applications pour lutter efficacement contre les bots qui visent leurs applications. Faute de protections adéquates, elles se feront inévitablement pirater et, parfois, de façon répétée.

D'après notre enquête, les personnes interrogées appartenant à des entreprises ayant fait l'objet de plusieurs violations étaient le plus souvent d'accord avec cette affirmation, ce qui laisse à penser que les bots sont probablement à l'origine d'un grand nombre d'entre elles.

La diversité des attaques de bots capables d'exploiter les vulnérabilités de nos applications rend la lutte contre celles-ci de plus en plus difficile

(n=750)



Les attaques de bots

CONSTATATION N° 5

Les attaques basées sur les bots ont été la cause première des violations de sécurité réussies contre les applications au cours des 12 derniers mois.

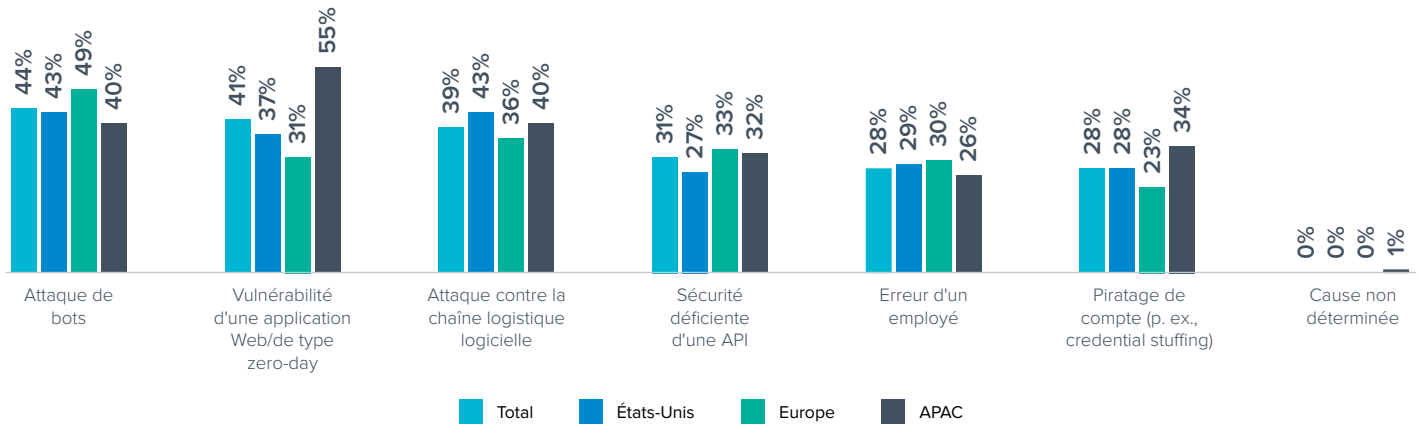
Les inquiétudes suscitées par les bots sont parfaitement légitimes, dans la mesure où ils ont été à l'origine de nombreuses violations d'application au cours de l'année écoulée. Toutefois, ils ne sont pas les seuls responsables.

En moyenne, les personnes interrogées ont imputé deux facteurs à la dernière violation subie par leur entreprise, ce qui témoigne de l'ampleur du problème.

La situation devient encore plus préoccupante si l'on considère que plus d'un quart (28 %) des personnes interrogées indiquent qu'une erreur d'un employé a joué un rôle dans celle-ci. Les entreprises peuvent bien mettre en place autant d'outils de sécurité qu'elles le souhaitent, si un employé commet une erreur qui laisse la porte ouverte aux pirates, alors ces derniers ne tarderont pas à exploiter cette vulnérabilité, que ce soit par le biais de bots, de la chaîne logistique logicielle ou d'autres moyens.

Parmi les éléments suivants, lesquels ont contribué à la réussite de la violation de sécurité ayant touché l'une des applications de votre entreprise au cours des 12 derniers mois ?

(n=541)



Les attaques de bots

CONSTATATION N° 6

La diversité des attaques de bots qui ciblent les applications fait qu'il devient difficile de les bloquer.

Avec autant de variété dans ce vecteur d'attaque, il n'est pas surprenant que tant d'entreprises aient du mal à défendre leurs applications contre les bots.

Alors que le spam provenant de bots constitue plutôt une nuisance, il est souvent utilisé pour dissimuler une activité plus malveillante, d'où la nécessité de s'en occuper fermement et non de le laisser courir. En fonction de sa fréquence et de son origine, ce spam peut vite prendre des proportions inquiétantes et facilement mettre en péril les activités de l'entreprise.

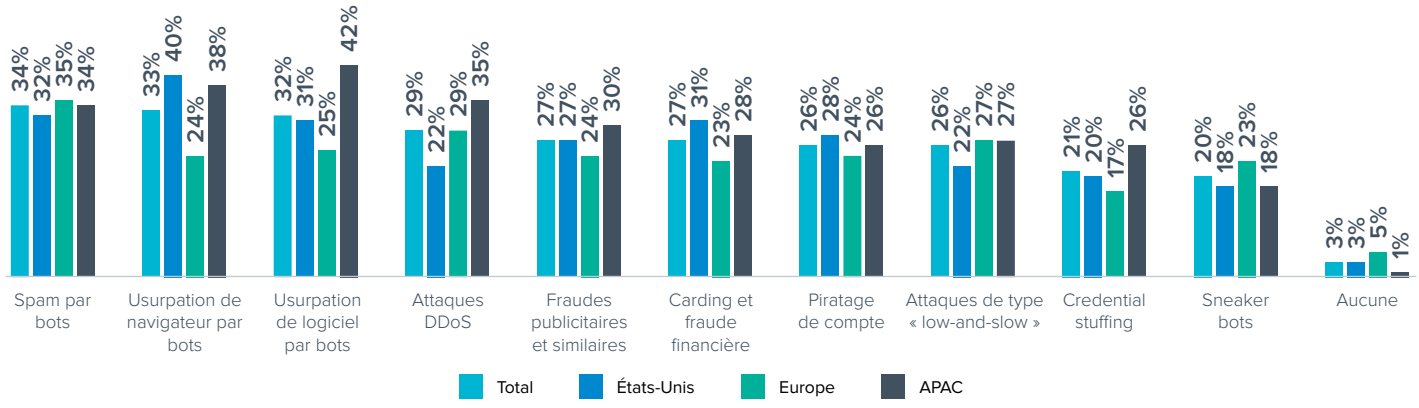
Les bots qui usurpent les navigateurs et les applications constituent également un problème majeur. D'un utilisateur essayant de dissimuler son véritable navigateur, à des bots exécutant des versions compromises d'applications dans des fermes à clics à des fins de fraude publicitaire ou à d'autres fins malveillantes.

Or la combinaison de ces bots augmente leurs chances de réussite. Les attaques de bots multivecteurs de type « low-and-slow » constituent le cœur du problème et ont très probablement contribué à certaines violations réussies l'an dernier.

On observe quelques disparités régionales intéressantes. La région Asie-Pacifique est la plus préoccupée par les attaques DDoS, dépassant de loin les autres régions et la moyenne mondiale. La principale préoccupation aux États-Unis et dans la région Asie-Pacifique sont respectivement l'usurpation de navigateur et l'usurpation de logiciel. En Europe, les sneaker bots retiennent une attention particulière.

Contre quels types d'attaques de bots visant les applications votre entreprise peine-t-elle à se défendre ?

(n=750)



Les attaques de bots

CONSTATATION N° 7

La prévention, la détection et l'identification des bots seront des fonctionnalités critiques pour les fournisseurs qui aident les entreprises à se défendre contre ce type d'attaques.

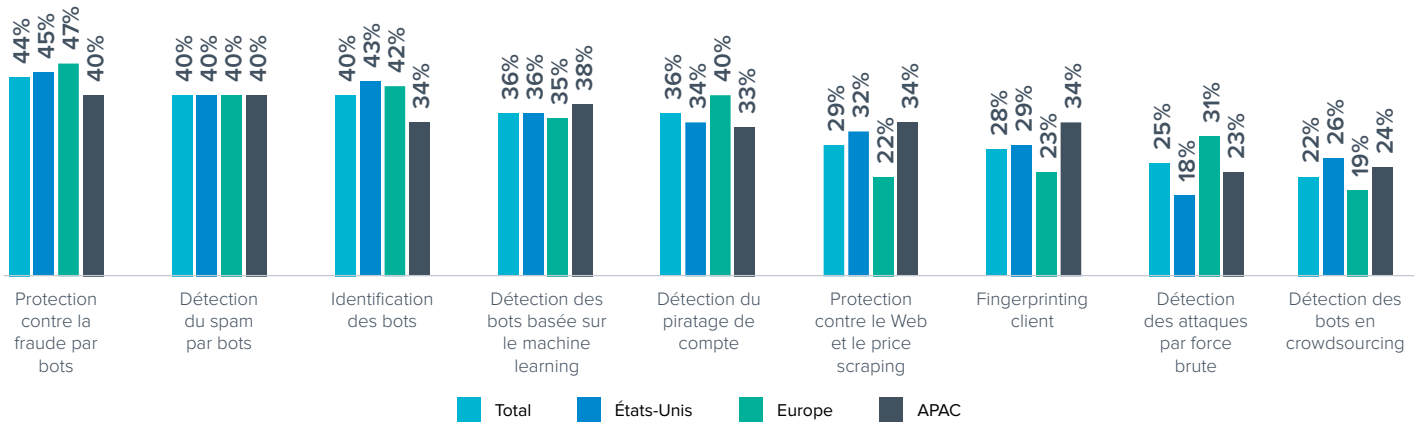
Que les entreprises soient confrontées à des bots frauduleux, de spam ou capables d'usurper des logiciels et des navigateurs, il est impératif qu'elles renforcent leurs défenses contre ce type d'attaques. En effet, les bots ont été la première cause de violation des applications au cours de l'année écoulée. Concernant le choix d'une solution de sécurité permettant de lutter contre les bots, trois domaines se détachent nettement dans notre enquête : la protection contre la fraude, la détection du spam et l'identification des bots.

Ces fonctionnalités sont essentielles pour se défendre contre la plupart des types d'attaques, mais tout fournisseur capable de les réunir au sein d'une seule et même solution améliorera considérablement le niveau de protection contre les bots de la plupart des entreprises.

Dans ces deux constatations clés, l'Europe considère invariablement la détection du piratage de compte et la détection des attaques par force brute comme plus importantes que les États-Unis et l'Asie-Pacifique. Ce phénomène s'explique probablement par les dispositions relatives à la protection de la vie privée et par le coût d'une intrusion prévus par le RGPD. Le fait que ces attaques soient menées par des bots de type « low-and-slow » les rend également difficiles à combattre.

Quelles fonctionnalités votre entreprise juge-t-elle les plus importantes dans le choix d'une solution de sécurité afin de protéger ses applications contre les attaques de bots ?

(n=750)



La sécurité des API

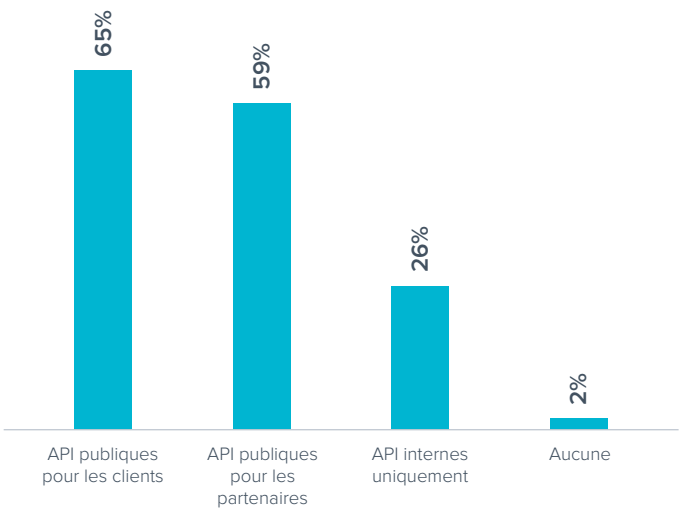
CONSTATATION N° 8

La généralisation des API publiques impose qu'elles soient correctement sécurisées.

Un pourcentage assez élevé des entreprises interrogées déploient des API publiques pour leurs clients (B2C) et leurs partenaires (B2B), ce qui montre qu'une majorité d'entre elles orientent leur développement vers les API. En effet, les API accélèrent le développement de nouvelles versions et améliorent la convivialité des applications. Problème : elles offrent également un formidable nouveau champ d'attaque aux cybercriminels. Les API insuffisamment sécurisées ont contribué à d'importantes violations de données au cours des deux dernières années. Il est donc primordial que les entreprises sécurisent leurs API de manière complète et efficace.

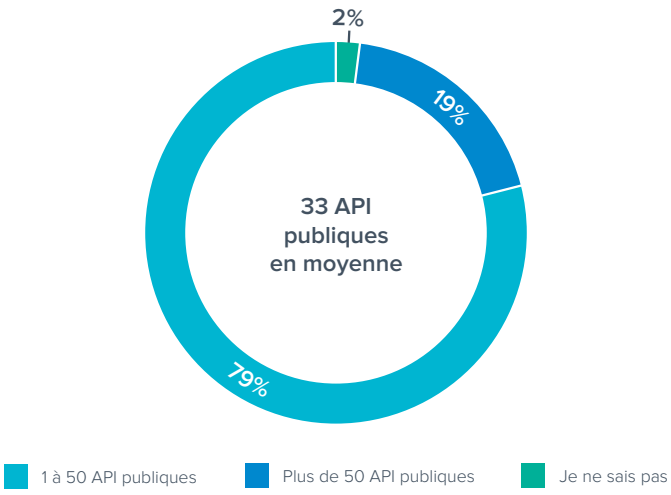
Quels types d'API votre entreprise utilise-t-elle ?

(n=750)



Combien d'API publiques votre entreprise utilise-t-elle ?

(n=642)



La sécurité des API

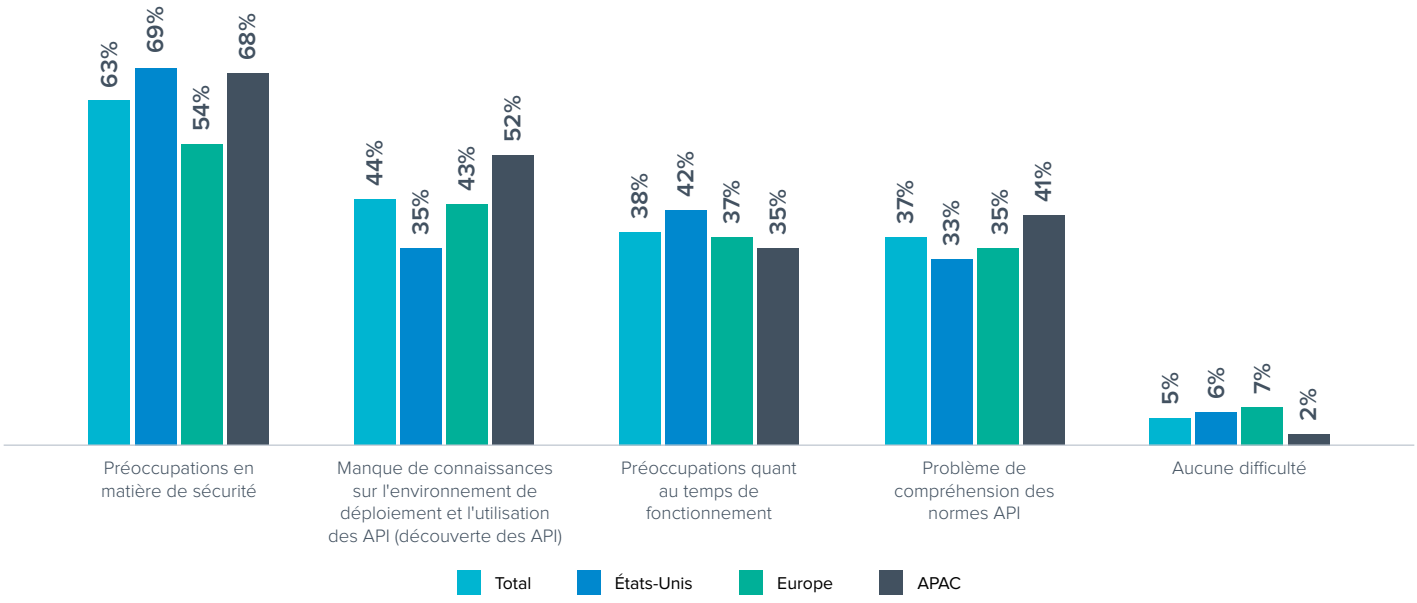
CONSTATATION N° 9

La sécurité des API est au cœur des préoccupations.

Sans surprise, lorsqu'il s'agit de déployer des API, les décideurs du monde entier considèrent la sécurité comme étant le plus important défi à relever. En raison de son système de déploiement avec accès direct à l'ensemble de ses données sensibles, une application basée sur un modèle API est beaucoup plus exposée qu'une application Web traditionnelle. Il va sans dire que le manque de connaissances autour du déploiement et de l'utilisation des API, ainsi que des normes qui les encadrent, viendront nourrir davantage ces inquiétudes.

Quelles principales difficultés votre entreprise rencontre-t-elle lors du déploiement d'API ?

(n=728)

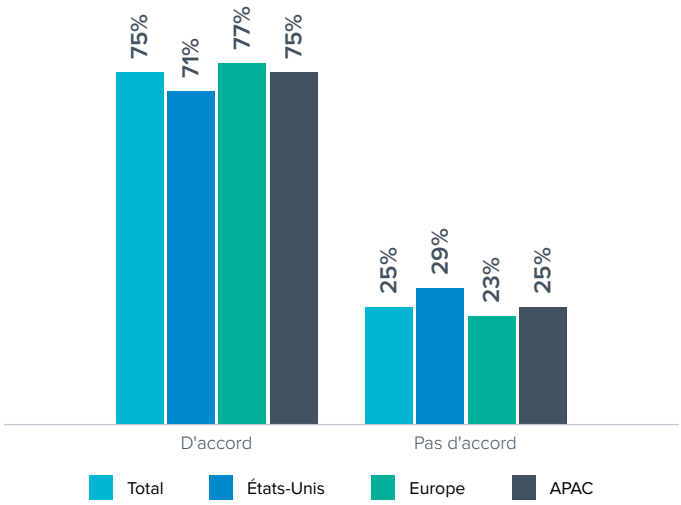


Les entreprises se sont ruées vers les API, en raison des avantages qu'elles offrent, mais la sécurité a pris un train de retard. Cet écart présente une aubaine pour les pirates qui ont alors la possibilité d'exploiter les failles présentes. Cette négligence est due à un manque de connaissances concernant la sécurité des API, à des erreurs de configuration ou des erreurs humaines, à la fausse croyance selon laquelle l'utilisateur final ne saura pas qu'une API fonctionne en arrière-plan et dans de très nombreux cas, au déploiement public d'API de test par les équipes en charge des applications, avec un accès direct et non sécurisé aux données de production.

Nous avons également demandé aux participants si l'utilisation d'API représentait un défi en matière de sécurité pour leur entreprise. 75 % ont répondu par l'affirmative. La plupart d'entre eux ont conscience des risques liés aux API, ce qui s'avère positif pour la sécurité des API à l'avenir.

L'utilisation d'API a soulevé des problèmes de sécurité pour mon entreprise

(n=728)



La sécurité des API

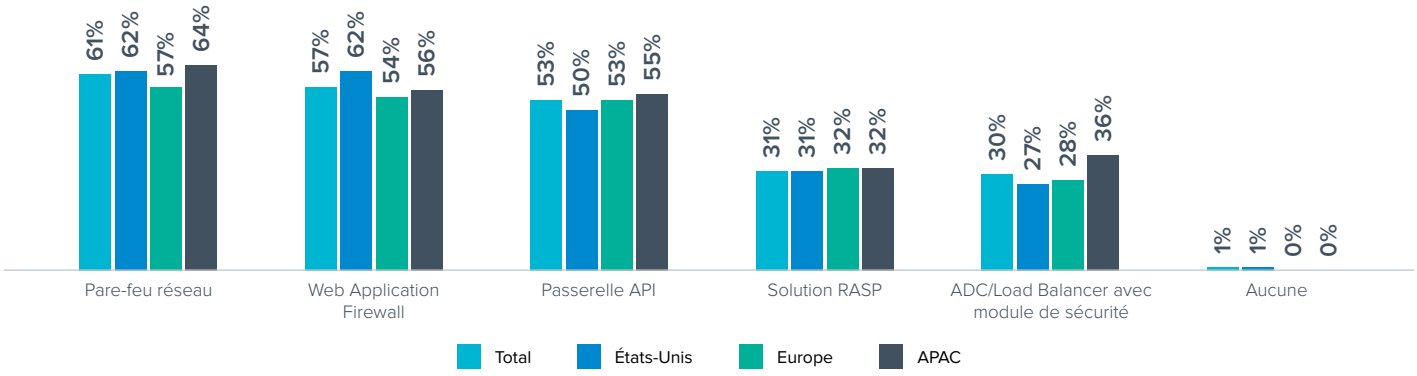
CONSTATATION Nº 10

De nombreuses entreprises ont adopté des solutions pour sécuriser leurs API (aussi bien pour le trafic entrant-sortant qu'entre les API), mais la plupart pensent que d'importantes améliorations restent à faire.

En moyenne, les entreprises ont recours à plus d'un outil pour sécuriser le trafic de leurs API. Pour autant, leurs préoccupations en matière de sécurité des API n'ont pas disparu, signe que les solutions actuellement utilisées n'offrent pas le niveau de sécurité attendu ou qu'elles ne s'intègrent pas correctement pour sécuriser totalement les API. En effet, la sécurité des API est encore en plein développement et la plupart des solutions utilisées pour protéger les API ne répondent pas encore à tous les besoins. À l'instar des pare-feux réseau, qui permettent uniquement de bénéficier d'une sécurité par reconnaissance de signature, d'une limite de débit ou d'un contrôle des accès basés sur l'adresse IP pour les API. Ils ne permettent pas d'appliquer une sécurité positive pour l'API ou d'importer les caractéristiques d'une API afin d'en configurer automatiquement les commandes. Les passerelles API fonctionnent très bien au niveau de la gestion d'API/gestion du trafic, mais leurs outils n'offrent pas toujours une couche de sécurité complète pour les API. Il est donc intéressant d'observer la manière dont les entreprises font évoluer leurs approches de protection multicouche pour les API. Beaucoup d'améliorations restent toutefois à faire.

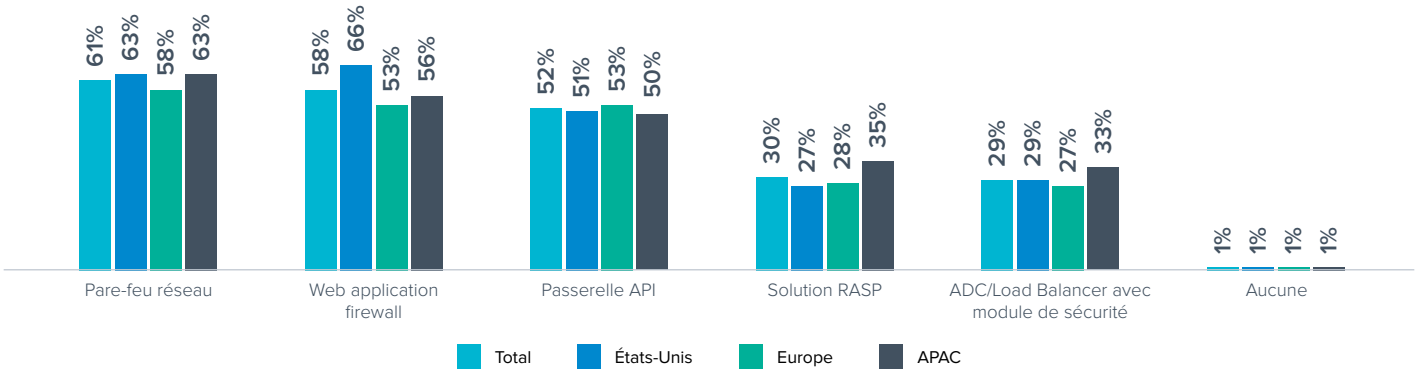
Quelles solutions votre entreprise utilise-t-elle pour sécuriser le trafic API nord-sud (entrant-sortant) ?

(n=728)



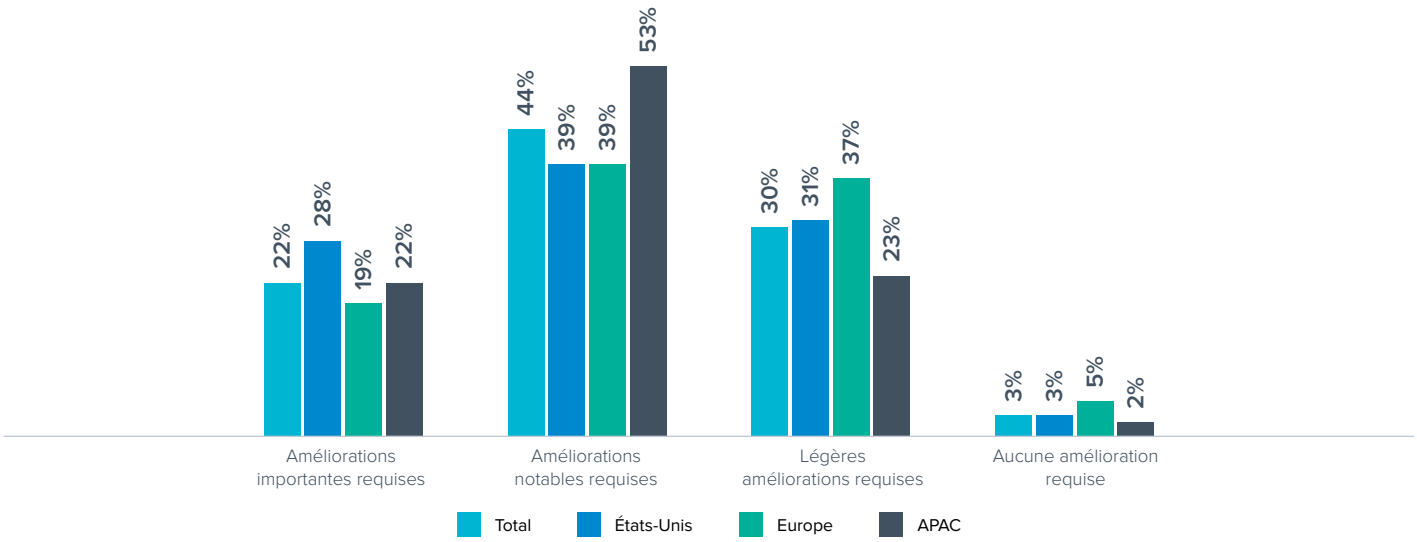
Quelles solutions votre entreprise utilise-t-elle pour sécuriser le trafic API est-ouest (application-application et API-API) ?

(n=728)



Selon vous, de quel niveau d'amélioration votre entreprise a-t-elle besoin dans le domaine de la sécurité des API ?

(n=728)



Les attaques contre les chaînes logistiques

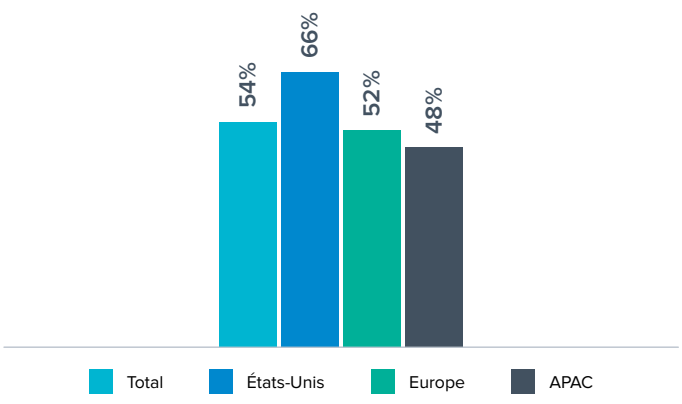
CONSTATATION N° 11

De nombreuses entreprises ont recours à des scripts tiers pour leurs applications Web et utilisent différentes méthodes pour les transmettre à un navigateur.

Encore une fois, l'efficacité est un point crucial lorsqu'il s'agit de développer des applications. En effet, en moyenne, plus de la moitié des entreprises utilisent des scripts tiers prêts à l'emploi pour leurs applications Web. Par conséquent, la sécurité devrait être au cœur de leurs préoccupations, en particulier lorsqu'une plateforme source telle que GitHub envoie directement du code à un navigateur. Si le code a été altéré, il se peut qu'une attaque de la chaîne logistique de type Magecart se prépare. Les entreprises doivent donc se méfier de cette approche pour ce qui est du développement des applications.

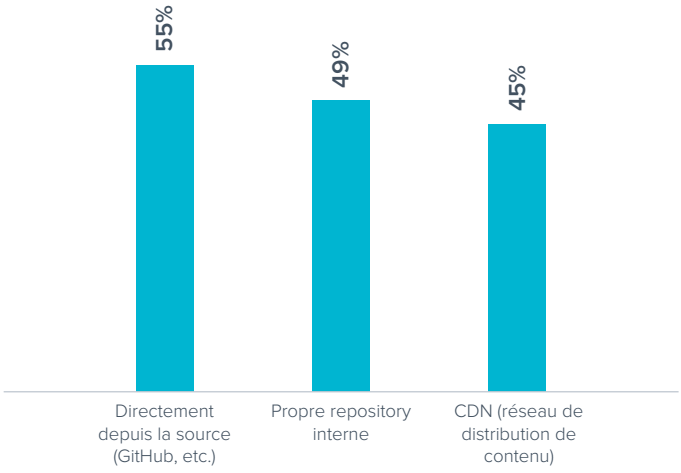
De manière approximative, quel pourcentage des applications Web de votre entreprise a recours à des scripts tiers ?

(n=750)



De quelle manière les sites Web de votre entreprise transmettent-ils des scripts côté client à un navigateur ?

(n=750)



Les attaques contre les chaînes logistiques

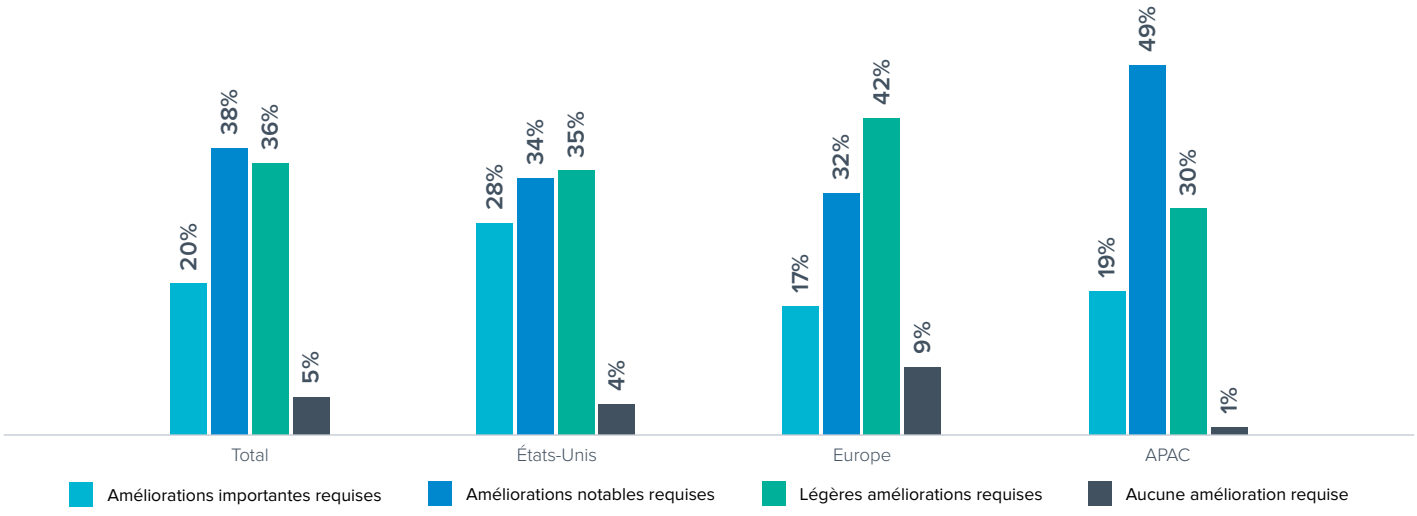
CONSTATATION Nº 12

Toutes technologies de protection contre les attaques de la chaîne logistique confondues, les participants sont conscients des améliorations que leur entreprise doit effectuer dans ce domaine.

Les attaques contre les chaînes logistiques logicielles ne cessent de se perfectionner : certains scripts sont même capables de désactiver l'exécution d'un code malicieux s'ils détectent qu'un scanner de vulnérabilités Web est en cours de fonctionnement, ce qui les rend extrêmement difficiles à contrer. Le champ des menaces, déjà en évolution constante, gagne une nouvelle fois en complexité. Bien que les entreprises déploient toute une gamme de technologies pour se protéger, ce vecteur d'attaque, tout comme les attaques de bots, semble toujours posséder une longueur d'avance. En outre, à la suite des dernières violations très médiatisées, la plupart des régions ont conscience que des améliorations doivent être apportées pour lutter contre les attaques qui visent les chaînes logistiques logicielles.

De quel niveau d'amélioration votre entreprise a-t-elle besoin pour lutter contre les attaques qui visent la chaîne logistique logicielle ?

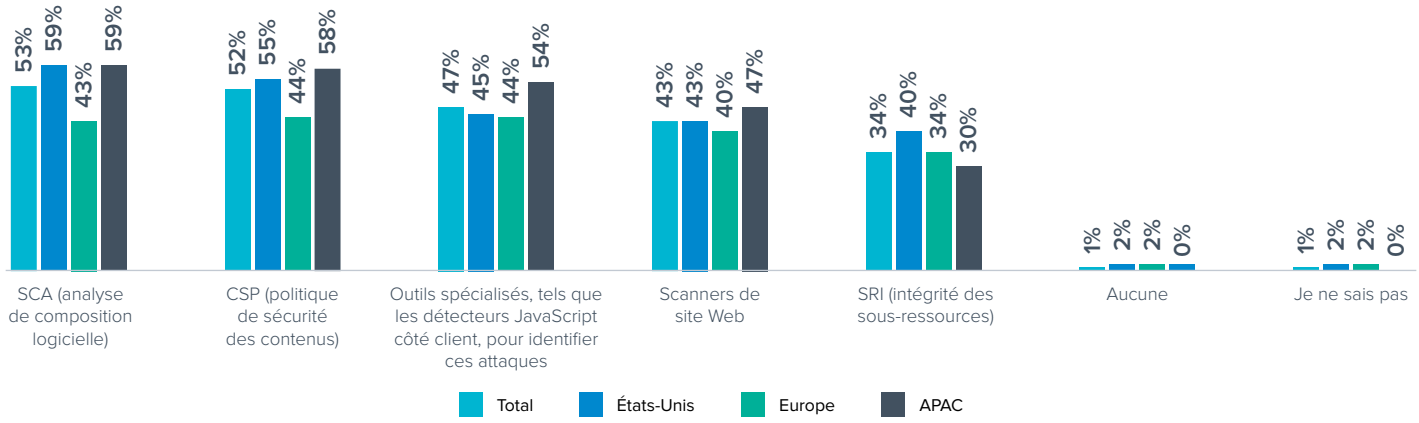
(n=750)



Des mesures de protection relativement standard sont en place pour réduire les attaques contre les chaînes logistiques. Par rapport à d'autres régions du monde, les participants de la région APAC ont davantage recours à des outils spécialisés (dont les détecteurs JS côté client) pour identifier des attaques. De tels détecteurs s'avèrent plus performants que des scanners de site Web pour identifier les attaques plus avancées. En effet, même si les scanners de site Web représentent la quatrième technologie la plus utilisée sur cette liste, ils sont facilement déjoués, comme le prouve le skimmer Baka détecté par Visa. En revanche, la SRI (intégrité des sous-ressources) est une technologie compliquée à configurer et entretenir, ce qui pourrait expliquer sa faible popularité.

Quelles technologies votre entreprise utilise-t-elle pour se protéger des attaques contre la chaîne logistique logicielle ?

(n=750)



Conclusion

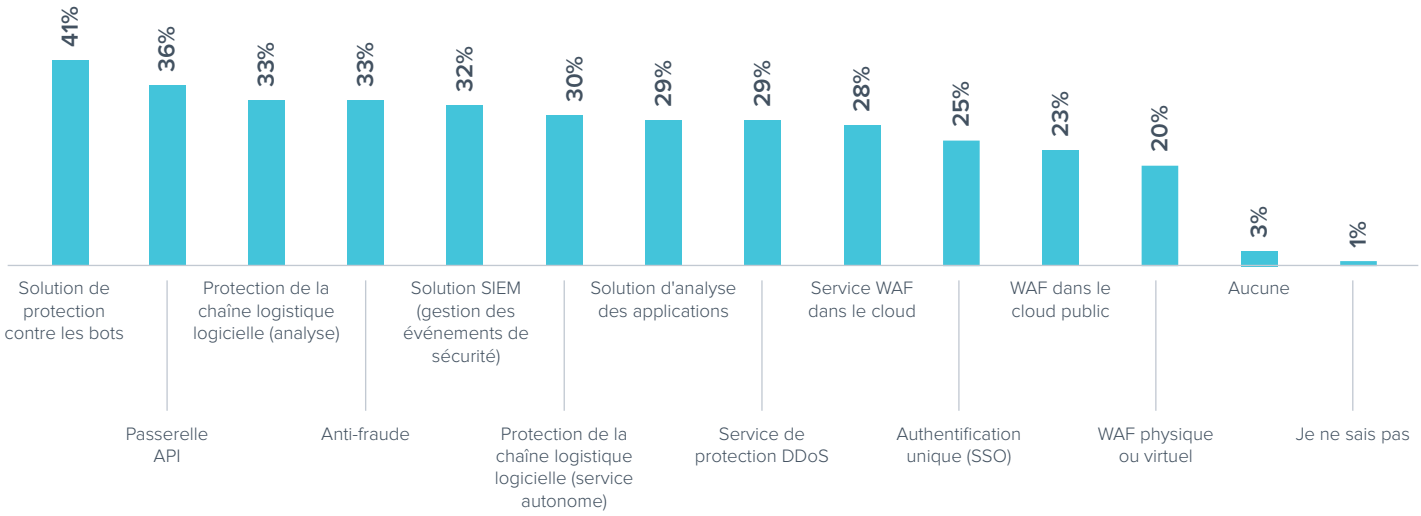
Compte tenu du grand nombre d'entreprises qui ont connu des intrusions au cours des 12 derniers mois par le biais de leurs applications Web, il est évident que des mesures supplémentaires doivent être prises pour se protéger de ces menaces, en particulier pour lutter contre les nouvelles menaces comme les bots et les attaques visant les API et les chaînes logistiques.

Les entreprises le savent, puisque nombre d'entre elles cherchent à déployer de nouvelles solutions dans les années à venir, dont une protection contre les bots (41 %), des passerelles API (36 %) et une protection des chaînes logistiques logicielles (analyse) (33 %).

Il s'agit d'un signe encourageant, mais plus les entreprises adoptent de solutions, plus la sécurité des applications gagne en complexité. Pour offrir une protection efficace, une solution de sécurité des applications doit se présenter comme une plateforme capable de protéger les clients contre tous ces vecteurs d'attaques. En effet, une approche de la sécurité des applications par plateforme permet d'obtenir une protection efficace aussi bien contre les menaces traditionnelles qu'émergentes, tout en restant simple à utiliser et gérer.

Parmi les solutions suivantes, laquelle sera déployée par votre entreprise l'année prochaine ?

(n=750)



Barracuda en quelques mots

Notre objectif : faire du monde un endroit plus sûr.

Chez Barracuda, nous pensons que chaque entreprise mérite un accès à des solutions de sécurité cloud de niveau professionnel, à la fois abordables, intuitives et facilement déployables. Nous protégeons vos e-mails, réseaux, données et applications à l'aide de solutions innovantes capables de s'adapter au parcours de nos clients et de se développer en conséquence.

Plus de 200 000 entreprises aux quatre coins du monde font confiance à Barracuda pour les protéger, même lorsque le danger ne leur semble pas imminent : nous nous voulons invisibles afin de permettre aux entreprises de se concentrer sur leurs activités et leur développement.

Pour en savoir plus, rendez-vous sur barracuda.com.

Barracuda®
Your journey, secured.