Cybersécurité : "il est temps de faire preuve de transparence envers les clients !"

Selon une étude du Ponemon Institute pour Intel, les entreprises préfèrent des fournisseurs transparents sur leurs produits, cela instaure un climat de confiance. En effet, le secret nuit aussi bien aux clients qu'au secteur de la cybersécurité. Une tribune proposée par Eric Fourrier, CEO de GitGuardian.

Temps de lecture : minute

1 novembre 2023

Lorsque les clients évaluent un produit logiciel, ils manifestent généralement des attentes avant l'achat, telles que : savoir en quoi consiste le produit, comprendre globalement comment il fonctionne, connaître le coût du produit, pouvoir l'essayer avant de l'acheter. Excepté dans le domaine de la cybersécurité, où peu d'informations sont transmises aux clients. La documentation sur les produits est cachée, le détail des prix reste confidentiel et pour essayer un produit il est nécessaire de signer un accord de confidentialité suivi d'un processus de qualification.

Comment expliquer ce niveau de confidentialité au sein du secteur de la cybersécurité ? Et pourquoi attendre des clients qu'ils continuent à la supporter ? Il n'est avantageux pour personne que des vendeurs de solutions de sécurité indispensables dressent des obstacles à leur compréhension. Trop de fournisseurs attendent de leurs clients qu'ils leur fassent confiance, alors même qu'ils ne sont guère disposés à prendre les mesures nécessaires pour instaurer cette confiance.

La confiance est compromise

Personne n'attend des fournisseurs qu'ils divulguent des informations sensibles sur la propriété intellectuelle. Toutefois, pour améliorer la situation du secteur, et garantir que les clients soient convaincus par l’engagement des entreprises face à la prévention des cybermenaces, il est impératif de renforcer la transparence.

Il est désormais courant pour les fournisseurs dans l’industrie d'exiger des prospects qu'ils signent des accords de confidentialité pour obtenir ne serait-ce que des informations de base, comme la prise en charge des interfaces de programmation (API) par un produit.

Exiger que des clients potentiels surmontent ces obstacles est évidemment mauvais pour eux, mais aussi pour le secteur. En retenant volontairement les informations relatives à un produit, la confiance est compromise, car les clients se demandent ce qu’il y a à cacher. Par ailleurs, plus les clients se heurtent à des obstacles, plus ils ont besoin de temps pour ajouter une protection de cybersécurité, et plus ils restent vulnérables à des attaques qui auraient pu être évitées.

Il faut proposer des essais gratuits des produits de cybersécurité

Pour instaurer la confiance, les fournisseurs de cybersécurité devraient être plus nombreux à proposer des démonstrations pratiques de leurs produits, avec des données réelles provenant du périmètre du client s'il l'autorise, sans accord de confidentialité (sauf si l'accord est exigé par le client). Mieux encore, les fournisseurs devraient proposer des essais gratuits de leurs solutions (y compris avec toutes les fonctionnalités), afin que les clients puissent les tester dans des conditions réelles avant de les acheter.

Il est impossible d'instaurer un climat de confiance si les clients pensent être dupés. Cependant, comment les clients peuvent-ils avoir confiance lorsque les vendeurs évitent de divulguer leurs tarifs avant d'engager un long processus de vente ? Ou, pire encore, lorsque les prix fluctuent fortement en fonction de la volonté du vendeur de conclure l'affaire ?

L'une des stratégies les plus efficaces pour renforcer la confiance des clients est de leur communiquer d'emblée les prix, avec des remises standards qu'ils peuvent calculer eux-mêmes. Étant donné que de plus en plus de fournisseurs dans le secteur de la sécurité optent pour une tarification plus secrète, la transparence se révèle comme la solution pour se démarquer.

Chaque entreprise exprime sa mission, mais combien y croient vraiment ? Cette question est particulièrement importante dans le domaine de la cybersécurité, dont la mission globale est de rendre le monde numérique plus sûr. Par exemple, des développeurs indépendants sont tout aussi vulnérables aux cybermenaces que des grandes entreprises, mais n’ont pas les moyens d’investir dans des produits destinés aux entreprises. Que doivent faire les fournisseurs de cybersécurité pour ces développeurs ?

Il y aura toujours un grand nombre d'utilisateurs qui pourraient contribuer de manière significative à rendre les espaces numériques partagés plus sûrs, mais pour lesquels les produits et les prix des entreprises ne sont tout simplement pas viables.

Proposer une version gratuite d'un produit aux utilisateurs, généralement des particuliers et des petites entreprises, peut être le moyen le plus efficace de faire avancer la mission d'un fournisseur. Une version gratuite est la meilleure démonstration à offrir. Elle renforce l’image de marque, accroît l'utilisation et permet de recueillir davantage de commentaires de la part des clients afin d'améliorer continuellement les produits.

En créant une entreprise avec des personnes investies dans leur mission, celle-ci a toutes les chances de rassembler une équipe de collaborateurs ambassadeurs. Souvent, ils sont tout aussi passionnés par l'éducation des clients que par la conception de produits. Cette passion peut également être un excellent indicateur de la philosophie et de l'approche globales d'un fournisseur de cybersécurité.

Les clients reconnaissent les fournisseurs qui veulent juste vendre leurs produits

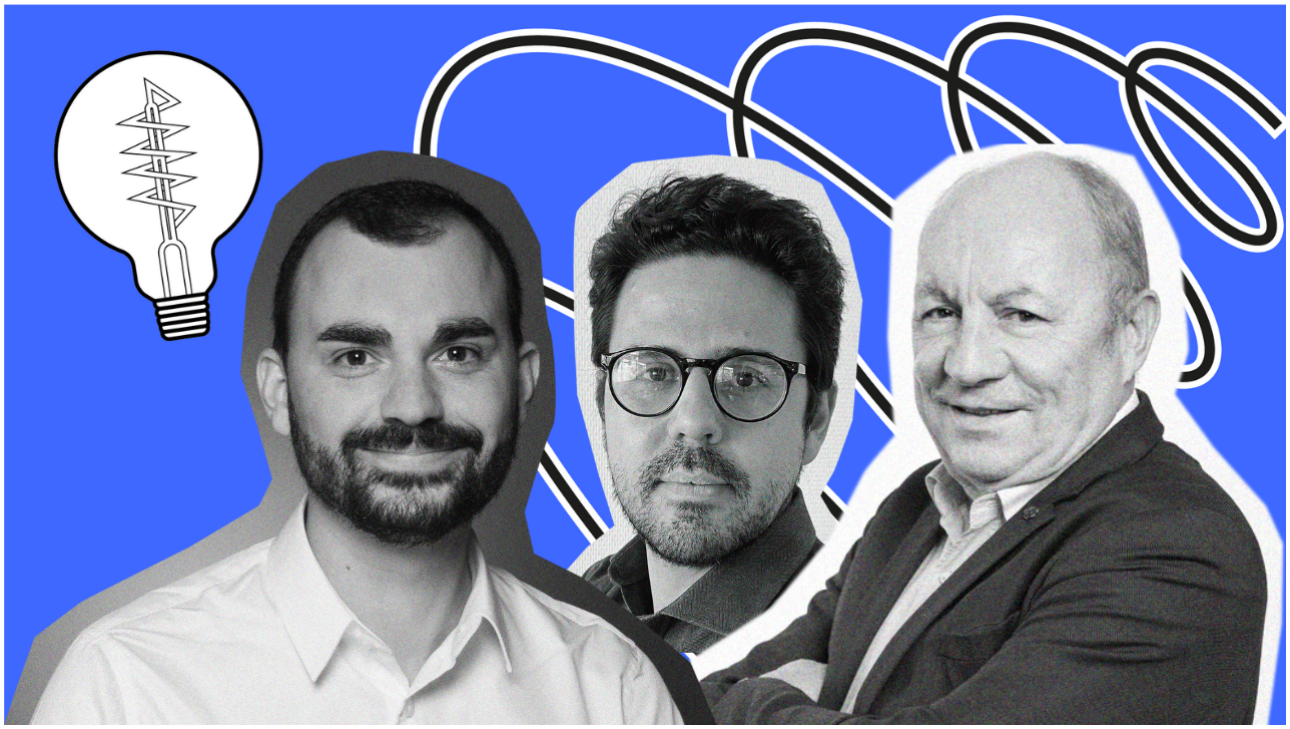
Les clients assistent à des conférences et à des événements. Ils savent reconnaître les fournisseurs qui sont présents uniquement pour vendre leurs produits. Ils peuvent aussi discerner quand les présentateurs croient vraiment en ce qu'ils font et cherchent à éduquer le marché sur des problèmes qu'ils considèrent comme extrêmement importants, qu'ils s'adressent à des clients potentiels ou non.

Une fois de plus, il s'agit d'une approche vertueuse, car de nombreux clients découvrent les fournisseurs grâce à ces présentations, même lorsque les conférenciers ne font pas allusion aux produits. Partager sa compréhension profonde des problèmes de l'industrie et sa passion pour les résoudre peut s'avérer plus efficace que n'importe quelle publicité.

D'un certain point de vue, on peut comprendre pourquoi les fournisseurs de cybersécurité optent pour le secret. En divulguant davantage d'informations, des concurrents pourraient avoir une meilleure connaissance des produits. Mais lorsque l'on a confiance dans la stratégie, la vision, les collaborateurs et la technologie, cette divulgation ne constitue pas une grande menace.

Mais pour que des clients accordent leur confiance, la transparence ne peut que favoriser cet objectif. Elle envoie un message clair démontrant que rien n’est dissimulé. Elle montre que plus les clients en savent sur

l’entreprise, plus ils réalisent qu’ils font le bon choix.



À lire aussi
Pénurie de talents cyber : comment (vraiment) y remédier ?

Article écrit par Eric Fourrier