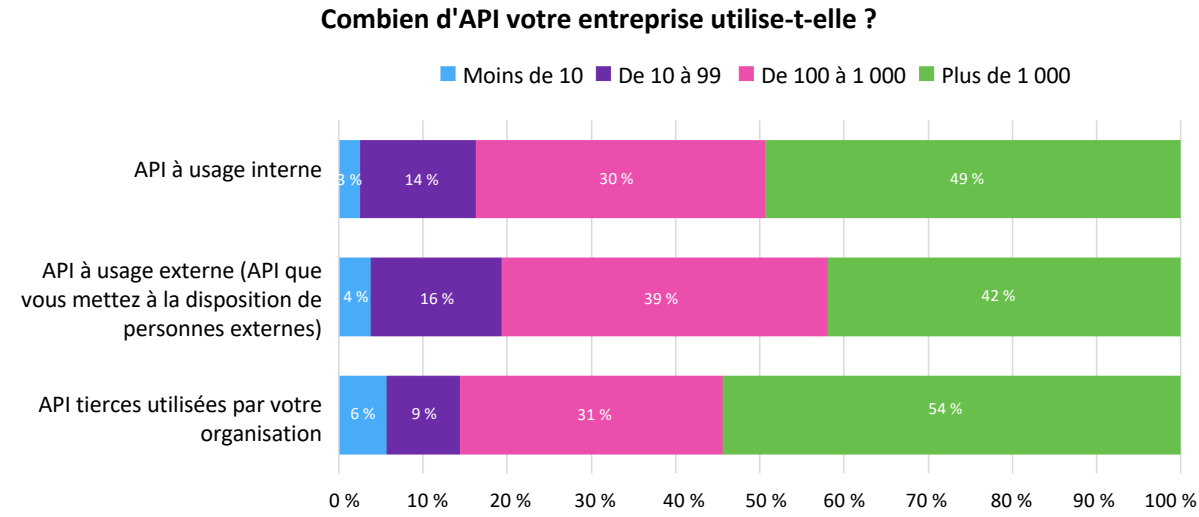
Figure 1 : Nombre d'API utilisées



Note : n = 160
Source : Omdia

L'utilisation des API est en hausse. Dans le même temps, de nombreuses personnes interrogées ont rapporté des incidents de sécurité des API, avec des problèmes spécifiques tels que l'exfiltration d'enregistrements internes et l'extraction de données à grande échelle.

L'augmentation du nombre d'API n'est pas prête de s'arrêter, et les entreprises doivent accroître dès maintenant leurs efforts pour les sécuriser. À défaut de mesures appropriées, les problèmes de sécurité ne vont cesser de s'aggraver. Au fur et à mesure que le nombre d'API augmente, la surface d'attaque continue à s'étendre, ce qui se traduit par la multiplication des attaques possibles.

Brève présentation de la sécurité des API

Le flux courant pour la sécurité des API se concentre autour de quatre principaux cas d'utilisation qui fonctionnent dans une boucle infinie, de façon assez semblable au cycle « build-ship-run-monitor » utilisé dans les flux de travail DevOps :

- **Découverte des API utilisées dans les différents environnements :** plusieurs méthodes sont disponibles, dont l'ingestion de définitions OpenAPI (Swagger), l'analyse des référentiels de code et l'analyse active des environnements. La plupart des API sont découvertes en analysant le trafic. Le téléchargement de fichiers de spécifications d'API est une tactique moins utilisée qui est possible uniquement lorsque l'entreprise connaît déjà les API qu'elle possède. En outre, une seule approche ne suffit pas : la combinaison de l'analyse continue du trafic et des référentiels peut permettre d'obtenir une vue complète de l'utilisation des API au sein des entreprises.