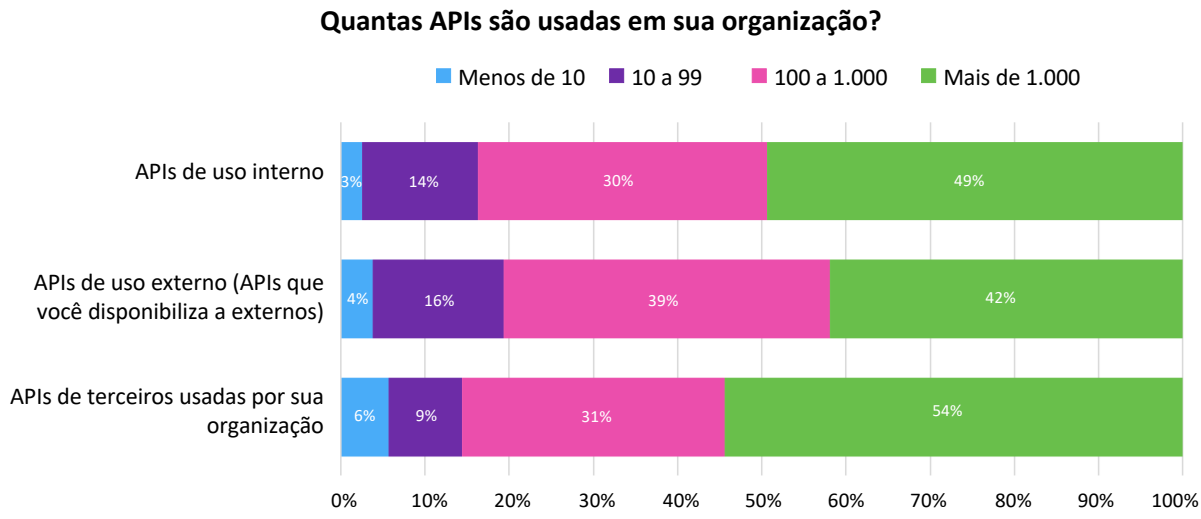
Figura 1: número de APIs em uso



Observação: n = 160
Fonte: Omdia

O uso de APIs está aumentando. Ao mesmo tempo, muitos de nossos participantes relataram incidentes de segurança de APIs com problemas específicos, como a exfiltração de registros internos e a extração de dados em larga escala.

Esse cenário mostra que as empresas devem melhorar seus esforços de segurança de APIs agora, pois o uso de APIs continuará a crescer, agravando os problemas de segurança, a menos que tais medidas sejam tomadas. Conforme o número de APIs aumenta, a superfície de ataque continuará a se expandir, resultando em uma possibilidade ainda maior de ataques.

Um guia rápido de segurança de APIs

O fluxo comum de segurança de APIs é centralizado em quatro casos de uso principais que operam em um loop infinito, de forma semelhante ao ciclo de "criação-envio-execução-monitoramento" usado no DevOps:

- **Descoberta das APIs usadas nos ambientes:** isso pode ser feito de várias maneiras diferentes, incluindo a ingestão de definições de OpenAPI (Swagger), a varredura de repositórios de código e a verificação ativa de ambientes. A maioria das APIs é descoberta pela análise do tráfego. O upload de arquivos de especificação de API é uma tática menos usada e só é possível quando a organização já sabe quais APIs ela tem. Além disso, uma única abordagem não é suficiente: a combinação do tráfego contínuo e da varredura de repositórios pode criar uma visão abrangente do uso de APIs dentro das organizações.

  As organizações precisam levar em conta as considerações de segurança de APIs em todo o seu patrimônio tecnológico, não apenas em ambientes específicos compatíveis com APIs. Em muitos casos, lidar com o uso de APIs legadas requer uma abordagem diferente.