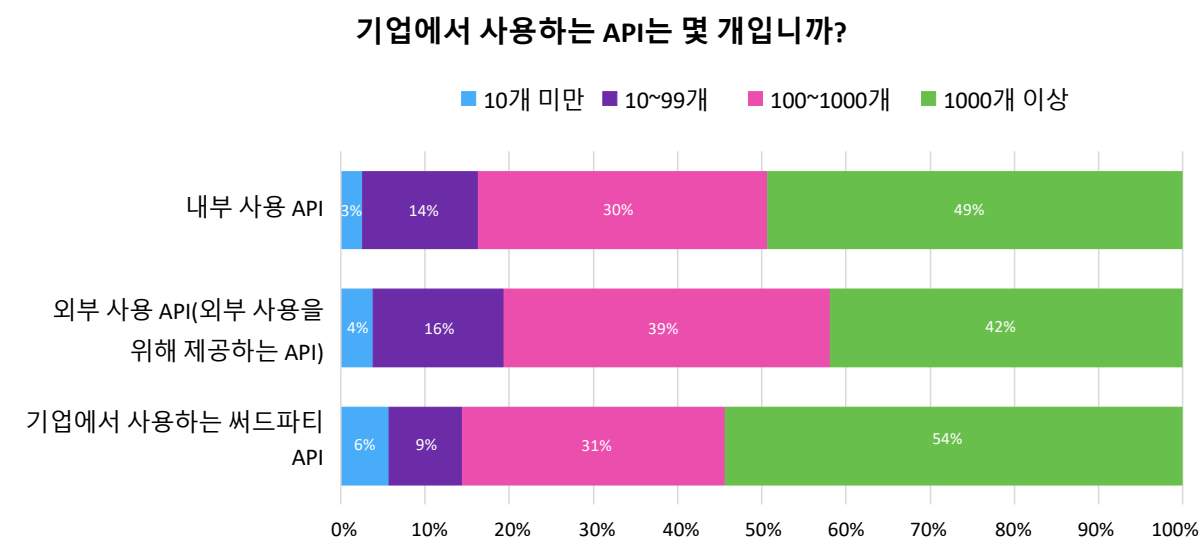
그림 1: 사용 중인 API의 수



참고: n=160
출처: Omdia

API 사용이 증가하고 있습니다. 동시에, 많은 응답자가 내부 기록의 유출과 대규모 데이터 스크레이핑 같은 특정 문제와 관련된 API 보안 인시던트를 보고했습니다.

이러한 시나리오를 고려하면 기업은 지금 API 보안 노력을 강화해야 합니다. 그렇지 않으면 API가 계속 증가하는 상황에서 보안 문제가 더욱 복잡해질 것이기 때문입니다. API의 수가 증가함에 따라 공격 표면은 계속해서 확대될 것이고, 그 결과 더 많은 잠재적 공격이 발생할 것입니다.

API 보안에 대한 간단한 입문서

API 보안의 일반적인 흐름은 DevOps에서 사용되는 제작-선적-운영-모니터링 사이클과 유사하게 무한 루프에서 작동하는 네 가지 주요 사용 사례를 중심으로 이루어집니다.

- **환경 전반에 걸쳐 사용되는 API 검색:** 이 작업은 OpenAPI(Swagger) 정의 수집, 코드 저장소 스캔, 환경의 능동적 스캔 등 다양한 방법으로 수행할 수 있습니다. 대부분의 API는 트래픽을 분석해 검색됩니다. API 사양 파일을 업로드하는 기법은 자주 사용되지 않으며 기업이 보유한 API를 이미 알고 있는 경우에만 가능합니다. 또한, 한 가지 접근 방식만으로는 충분하지 않습니다. 지속적인 트래픽과 저장소 스캔의 조합은 기업 내 API 사용에 대한 포괄적인 시각을 제공할 가능성이 높습니다.